Appendix 1 to Vespia OÜ Terms and Conditions (the "T&C")

DATA PROCESSING AGREEMENT

This data processing Agreement (**"DPA"**) is entered into between **Vespia OÜ** ("Vespia") and the Client, forms an inseparable part of the T&C and constitutes the data processing agreement between Vespia as a data processor and the Client as the data controller in the meaning of GDPR Article 28.

WHEREAS:

(A) Capitalized terms used in this DPA shall have the meaning ascribed to them in the T&C if not otherwise provided in this DPA;

(B) GDPR means the general data protection regulation ((EU) 2016/679), implemented since 25 May 2018.

NOW, THEREFORE the Parties have agreed as follows:

1. The Client acknowledges and agrees that any and all Client Data (including its lawfulness, quality, and accuracy) shall be the sole responsibility of the Client. The Client shall be solely responsible for uploading Client Data through the use of the Solution or making it otherwise available to Vespia for the use of the Solution.

2. In connection with Client Data, the Client confirms that: (i) it either owns its Client Data or has the necessary rights to use and authorize further use by Vespia as stipulated by the T&C and this DPA; (ii) it has the appropriate legal basis for the processing of the Personal Data and for authorizing Vespia to process the Personal Data in accordance with the T&C and the DPA.

3. The Client acknowledges and approves that Vespia may in an aggregated or anonymized format use the Client Data for Vespia's internal analysis with the aim to improve the quality of and develop the Solution by adding functionality, new features, etc.

4. The Client shall at all times ensure that processing of the Client Data by it is lawful and in compliance with applicable legal acts (including data protection laws). By uploading Client Data to the Solution or making it otherwise available to Vespia for the use of the Solution, the Client authorizes Vespia to process the Personal Data as stipulated in the T&C.

5. The Client hereby instructs Vespia to process the Personal Data as described in this DPA.

6. Upon processing the Personal Data Vespia shall:

    6.1. process the Personal Data only within the scope required according to the T&C and for provision of the Solution or in any other way according to the instructions of the Client;

    6.2. apply appropriate technical and organizational measures listed in Schedule 1 hereto (**List of applicable TOMs**) in order to protect the Personal Data against unauthorized or unlawful processing and accidental or unlawful loss, destruction, damage, alteration or disclosure; ensure the performance of the Personal Data protection laws; and ensure the protection of rights of data subjects;

    6.3. refer all requests or inquiries by data subjects (e.g. Client´s customers) to the Client without responding to such requests;

    6.4. keep the Personal Data confidential and guarantee that all employees of Vespia involved in the provision of Solution are bound by confidentiality obligation;

    6.5. transfer the Personal Data outside the EU only in compliance with conditions laid down in GDPR Chapter V;

6.6. make available information reasonably required by the Client to demonstrate the fulfillment of the obligations of the Client as the controller and Vespia as the processor on the basis of GDPR Article 28;

6.7. enable the Client or an expert authorized by the Client to perform the Personal Data processing and protection-related audits and contribute to their conduct;

6.8. immediately inform the Client of any data protection incident and take all measures required to remedy/mitigate the consequences of the data protection incident, unless the Client has advised otherwise;

6.9. assist the Client at the cost of the Client in fulfillment of the obligations stipulated in GDPR Articles 32-36, taking into consideration the method of processing of Personal Data and the information available for Vespia.

7. The Parties agree on the following:

7.1. Duration of the data processing - the duration of the data processing shall be the duration of the T&C;

7.2. Data subjects - the Personal Data processed may concern the following categories of data subjects: representatives and employees of the Client, Client´s customers/end-users (their representatives, employees, shareholders, and owners),;

7.3. Categories of data - the Personal Data processed may concern the following categories of data: name, e-mail address, date of birth, personal ID code, location, IP address, web browser version and type, screen type, and size, user's behavioral and application usage data, pictures and videos of a person and personal ID, bank statements and transactions, blockchain transactions and ledger records, blockchain wallet and smart contract numbers, place of residence, address, PEP status, international sanctions applied to a person, identification documents, utility bill info, other data obtained via the use of the Solution (incl. searches from private and public registries)

7.4. Purpose of processing operations - providing the Solution to the Client as described in the T&C.

8. By executing this DPA, the Client grants Vespia a general authorization (in the meaning of GDPR Article 28(2)) to involve sub-processors for the purposes of providing the Solution. Vespia shall by e-mail inform the Client of any intended changes concerning the addition or replacement of other sub-processors, thereby giving the Client an opportunity to object to such changes by notifying Vespia by e-mail within 7 days after receipt of respective notice from Vespia. If the Client objects to a new sub-processor, as permitted in the preceding sentence, Vespia will use reasonable efforts to make available to the Client use of the Solution in a way to avoid processing of Personal Data by the objected-to new processor without unreasonably burdening the Client. If Vespia is unable to make such change available within a reasonable period of time, which shall not exceed 30 days, the Client may terminate the T&C.

9. The sub-processors currently used by Vespia for provision of the Solution, *inter alia* for processing of the Personal Data are:

- NameScan (Australia) - partner for Sanctions, PEP, Adverse media checks. Any Personal Data transfers out of the EU are subject to the EU Commission's Standard Contractual Clauses.

- Amazon Web Services (AWS) – cloud computing services, data storing, by default the data is stored in the EU, if not agreed otherwise;

- Hotjar – a tool that Vespia uses to analyze the users' experience and understand how to optimize the Solution;

- Intercom – a tool that Vespia uses for support ticketing and support chart;
- Amplitude – a tool that Vespia uses to analyze the users' experience and understand how to optimize the Solution;
- Google Analytics – a tool that Vespia uses to analyze the location and sources where users come from, to improve marketing communication and targeting.
- Mailchimp/Mandrill app - a tool that Vespia uses for email automation and analysis.
- Hubspot – tool that Vespia uses to understand its website traffic to improve its marketing efforts.
- Google Tag Manager – a tool that Vespia uses to improve its conversion tracking, site analytics, remarketing, etc.
- Google Search Console – a tool that Vespia uses to monitor, maintain, and troubleshoot its site's presence in Google Search results.
- Google Optimize – a tool that helps Vespia monitor the results of experiments on web pages.

10. If Vespia uses sub-processors for carrying out specific processing operations with the Personal Data, it will do it based on the contract (including the data processing agreement) concluded with such processor.

11. During the validity of the T&C, Vespia will retain the Client Data obtained by the Client via the use of the Solution) for a retention period as applicable to the Solution package chosen by the Client.

12. Vespia will process Personal Data on behalf of the Client until the termination of the T&C. Upon termination of the T&C, Vespia will impersonate or obfuscate (one-way operations, not enabling re-personalization) all Client Data (incl the Personal Data) in accordance with the terms stipulated in the Solution package chosen by the Client (unless otherwise instructed by the Client), unless EU or Estonian law requires further storage of certain Personal Data.

13. Notwithstanding the provisions of this DPA, Vespia may disclose Client Data (incl Personal Data) to the extent obligated by applicable laws. In such case, Vespia will use reasonable efforts to provide Client with prior notice of such disclosure (to the extent legally permitted). Should the Client desire to contest the disclosure of the Client Data, it shall provide Vespia reasonable assistance, at the cost of the Client.

14. With regard to issues not regulated by the Parties in this DPA, e.g. governing law, resolution of disputes, liability, etc. the provisions of the T&C shall apply.

DPA Schedule 1 – List of applicable TOMs

Security Measures	
1.1.	**Access control to systems (virtual)**: The following technical and organizational measures are in place for user identification and authentication. ● Encryption of data in transit and at rest (covered by infrastructure and platform partner) ● Personal and individual user log-in when entering the system ● Additional system log-in for special applications ● Automatic blocking of the computer after a certain period of time without user activity (also password-protected screensavers or automatic pause function) ● User access logs
1.2.	**Access control to data**: The following measures are in place to ensure that data is accessed only by authorized employees in accordance with their access rights: ● Role-Based Access Control ● Authorization routines ● Reports/data logs (for technical, non-business purposes) ● Reviews / Audits (for technical, non-business purposes) ● Restricted use of removable media (e.g. external hard drives), encryption and authorization prior to using
1.3.	**Disclosure control**: The following measures are in place to ensure secure transport, transmission, communicate, or storage of data on data media (manual or electronic). ● It is not allowed to store any customers' data outside of infrastructure and platform partner ● Logging
1.4.	**Input control**: The following measures are in place for verifying and tracking whether data have been entered, changed, removed, or deleted, and by whom. ● Access rights ● System logs ● Security/logging software ● Functional responsibilities
1.5.	**Availability control**: The following measures are in place to assure data availability and protect against accidental destruction or loss of data. ● Back-up processes for technical (non-business) purposes (cloud storage and databases are used, which do not require backups) ● Retention of back-ups ● Customer might perform business purpose backups of data through API and set up the retention for backups ● Hosting service provider in compliance with ISO 27001, 27017, 27018, in addition to SOC 1, 2, and 3
1.6.	**Separation control**: The following measures are in place to ensure that data processed for different purposes are processed separately. ● Logical separation of client data within databases ● Encryption of client data in transit ● Separation of test, development, and production environments

To stay compliant, we have a strategic partner and use infrastructure, storage, and databases through Amazon Web Services. The data never leaves AWS servers.

Here is the list of security topics and the corresponding documents:

SOC 3 Report
https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf

CSA STAR LEVEL 1: CSA STAR Self-Assessment
https://d1.awsstatic.com/whitepapers/compliance/CSA_Consensus_Assessments_Initiative_Questionnaire.pdf

CSA STAR CCM v4.0
https://d1.awsstatic.com/certifications/csa_star_certification.pdf

ISO/IEC 27001 and 9001
https://d1.awsstatic.com/certifications/iso_27001_global_certification.pdf
https://d1.awsstatic.com/certifications/iso_9001_certification.pdf