Data Protection Agreement

This Data Protection Agreement ("**DPA**"), as amended from time to time, serves as an integral part of any kind of agreement, that this DPA is contained therein, such as SOW and License Agreement (the "**Agreement**"), entered into by and between Veego Software Ltd. or the Veego Software Affiliate party, in accordance with the Agreement (together "**Veego**") on behalf of itself and its Affiliates, and the counterparty of the Agreement, on behalf of itself and its Affiliates ("**Controller**"). Each of Veego and Controller is referred to individually as a "**Party**" and collectively as "**Parties**".

1. Background.

1.1. In the course of exercising its obligations under the Agreement, Veego processes personal data for or on behalf of the Controller;

1.2. By virtue of the Agreement and this DPA, Veego may process Personal Data on behalf of the Controller.

2. Interpretation; Definitions.

2.1. Unless otherwise defined herein, capitalized terms used in this DPA shall have the following meaning:

"**Affiliate**"	means any person or entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control" for the purpose of this definition means direct or indirect ownership or control of at least 50%.
"**Applicable Law(s)**"	means all applicable data protection and privacy and electronic marketing legislation, including Data Protection Act 2018, the EU Privacy and Electronic Communications (EC Directive) Regulation, the GDPR, the CCPA as well as any equivalent laws that may apply to the Controller's Personal Data to be processed hereunder by Veego.
"**CCPA**"	means the California Consumer Privacy Act of 2018 California Civil Code § 1798.100 et seq., as supplemented or amended by the California Privacy Rights Act of 2020. Under the CCPA, Veego qualifies as a service provider, and Veego agrees to comply with the requirements of service providers as described in the CCPA and as specifically described in this DPA.
"**EEA"**	means European Economic Area. In this DPA the EEA shall include the EU Member States and EEA member countries.
"**GDPR**"	means EU General Data Protection Regulation 2016/679 and any subsequent amendments, replacements, or supplements; the terms "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Special Categories of Data**", "**Process" or "Processing**", "**Controller**", "**Processor**", and "**Supervisory Authority**" shall have the same meaning given to them in the GDPR (or where the same or similar

terms are used under another Applicable Law, the meaning given to such terms under such Applicable Law.

"**Sensitive Personal Data**"	means a subset of Personal Data, which due to its nature has been classified by applicable law or by Veego as deserving additional privacy and security protection. Sensitive Personal Data consists of, in particular: (i) all government-issued identification documents and numbers (including Social Security numbers, driver's license numbers, and passport numbers); (ii) all financial information, including any consumer, trading or spending habits, and any account numbers (bank and non-bank financial services account numbers, credit/debit card numbers, and other information would permit access to a financial account); (iii) any Personal Data pertaining to the categories specified in Articles 9-10 of the GDPR; (iv) all employee, employment candidate, and payroll information and data; and (v) any other Personal Data designated by Veego as Sensitive Personal Data.
"**Sub-Processors**"	means any Processor engaged directly by Veego or any Veego Affiliate to process any Personal Data pursuant to or in connection with the Agreement. The term shall not include employees or contractors of Veego.
"**Veego Services**"	means any services provided by Veego to the Controller under the Agreement.

3. Scope of processing.

3.1. The Controller hereby instructs Veego to process Personal Data solely for the purpose of providing the Veego Services, unless applicable laws to which Veego is subject require such Processing. Veego shall process Personal Data as a Data Processor acting on behalf of the Controller of such Personal Data.

3.2. Veego shall process the Personal Data as described in **Annex 1** (details of Processing of Personal Data) attached hereto and in accordance with, (i) the terms of this DPA; (ii) the terms of the existing agreement between the Parties; (iii) the Controller's documented instructions, unless the processing is required by Applicable Laws; and (iv) all Applicable Laws.

3.3. Veego shall notify the Controller without undue delay if Veego determines that it can no longer meet the Controller's instructions or its obligations under this DPA.

3.4. The Controller warrants that its instructions at all times shall comply with applicable data protection and privacy legislation. The Controller furthermore warrants that it has an appropriate legal basis for the collection and processing of the Personal Data under this Agreement and DPA and is solely responsible for the legality of such Personal Data.

4. California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA)

4.1. To the extent any Controller Data is considered Personal Information (as such term is defined under the CCPA) and is subject to the CCPA, the parties agree that: (a) Veego shall not sell or share (as those terms are defined in the CCPA and other applicable Protection Laws; (b) Veego shall only use and process the Controller Personal Information on the Controller's behalf and solely pursuant to the terms set forth in the Agreement; (c) Veego may engage in "Business Purposes" within the scope of the CCPA, including the Business Purposes as defined in Sections 1798.140 (2)-(7).

4.2. Veego shall not (a) retain, use, or disclose Controller Personal Information for any purpose other than for the specific purpose of performing the Services or as otherwise expressly permitted under the Agreement including retaining, using or disclosing the Personal Information for a commercial purpose other than the business purposes specified in this DPA Terms or the Agreement, or as otherwise permitted by the CCPA; (b) retain, use or disclose the Controller Personal Information outside of the direct business relationship with the Controller; (c) combine the Controller Personal Information with personal information that it receives from or on behalf of a third party or collects from California residents, except that Veego may combine the Controller Personal Information to perform any business purpose as permitted by this DPA, the Agreement, or the CCPA or any regulations adopted or issued under the CCPA.

4.3. Veego shall assist the Controller to fulfill required obligations under the CCPA and to respond to requests from consumers exercising their rights under the CCPA (e.g., deletion and access), all in accordance with the CCPA requirements.

5. Veego's Personnel.

Veego shall take reasonable steps to ensure that all the Veego's employees or contractors ("**Veego Personnel**"): (i) have such access only as necessary for the purposes of providing the Veego Services and is acting in compliance with Applicable Laws; (ii) is contractually bound to confidentiality requirements no less onerous than this DPA; and (iii) is providing with appropriate privacy and security training, if and as required by Applicable Law.

6. Security.

6.1. Veego shall assess and implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk presented by the processing of Personal Data, as described in **Annex 2**, including:

6.1.1. The pseudonymization and/or encryption of Personal Data, which in the case of any Sensitive Personal Data, shall be encrypted in transit and at rest;

6.1.2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

6.1.3. The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

6.1.4. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

6.2. In assessing the appropriate level of technical and organizational measures, Veego shall take into consideration the risks that are presented by the Processing, including the risk of a Personal Data Breach, through accidental or unlawful loss, destruction, alteration, unauthorized disclosure of or access to the Controller's Personal Data.

6.3. Veego shall keep records of its processing activities performed on behalf of the Controller, which shall include:

6.3.1. The details of the Processor as Personal Data Processor, any representatives, Sub-Processors and the Veego Personnel having access to Personal Data;

6.3.2. The categories of Processing activities performed;

6.3.3. Information regarding cross-border data transfer, if any; and

6.3.4. Description of the appropriate technical and organizational security measures implemented in respect of the processed Personal Data.

7. Sub-processing.

7.1. Veego has the Controller's authorization for the engagement of Sub-Processors as available in the agreed list attached hereto as **Annex 3**. Veego shall inform the Controller in writing of any changes to the list through the addition or replacement of the Sub-Processor within thirty (30) days following such changes (the "**Engagement**"). The Controller may reasonably object to the Veego's use of a new Sub-Processor, for a reason relating to the protection of Personal Data intended to be processed by such Sub-Processor, by notifying Veego promptly in writing within fourteen (14) days after the Veego's notice.

7.2. Such written objection shall include those reasons for the objection to the Veego's use of such a new Sub-Processor. Failure to object to the Engagement in writing and on a timely manner shall be deemed as acceptance of the new Sub-Processor. In the event the Controller reasonably objects to an Engagement, Veego will use reasonable efforts to make available to the Controller a change in Veego Services so to avoid processing of Personal Data by the Sub-Processor to which the Controller objects, without unreasonably burdening the Controller. If Veego is unable to make available such change within thirty (30) days, the Controller may, as a sole remedy, terminate the applicable agreement and this DPA with respect only to those services which cannot be provided by Veego without the use of the Sub-Processor to which the Controller objected, by providing written notice to Veego. The Controller will have no further claims against Veego due to the termination of the Agreement and/or this DPA in the situation described in Article 7.

7.3. Where Veego engages Sub-Processors, Veego will take reasonable steps to impose on the Sub-Processors, by way of contract, data protection terms that provide at least the same material level of protection for Personal Data as those in this DPA (including, where appropriate, the Standard Contractual Clauses), to the extent applicable to the nature of the services provided by such Sub-Processors.

8. Data Subjects Rights.

8.1. The Controller is solely responsible for compliance with any obligations regarding the exercise of Data Subject Rights under applicable privacy legislation.

8.2. Taking into consideration the nature of the processing, Veego shall reasonably assist the Controller in responding to requests to exercise Data Subject rights under Applicable Laws, including EU Data Protection Laws.

8.3. Veego shall:

8.3.1. Promptly notify the Controller if it receives a request from a Data Subject in respect of Personal Data;

8.3.2. Provide cooperation and assistance where feasible in relation to any complaint or request from a Data Subject regarding the Processing of Personal Data at the Controller's sole expense;

8.3.3. Ensure that it does not respond to that request except on the documented instructions of the Controller or as required by Applicable Laws to which Veego is subject, in which case Veego shall to the extent permitted by Applicable Laws inform Controller of that legal requirement before it responds to the request;

8.3.4. Maintain electronic records of complaints or requests from Data Subjects seeking to exercise their rights (under Applicable Laws).

9. Legal Disclosure; Personal Data Breach.

9.1. Veego shall notify the Controller without undue delay of becoming aware of:

9.1.1. Any legally binding request for disclosure of Personal Data by a law enforcement authority unless otherwise prohibited by applicable laws and/or regulations;

9.1.2. a Personal Data Breach affecting Controller Personal Data, providing Controller with sufficient information (to the extent possible) to allow the Controller to meet any obligations to report or inform Data Subject or Data Protection Authorities of the Personal Data Breach under the Applicable Laws.

9.2. Veego shall cooperate with the Controller and take reasonable commercial steps as directed by the Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach, all in accordance with the demands of the Applicable Law at the Controller's sole expense.

9.3. Other than as required by law, Veego shall not make any public statements or other disclosures about a Personal Data Breach affecting Personal Data without the Controller's prior written consent, which is provided on a case-by-case basis.

10. Erasure or return Personal Data.

10.1. Within thirty (30) days after the Controller's written request, Veego shall erase, return or otherwise make unrecoverable and/or anonymized all copies of Personal Data, at the Controller's choice, except as required to be retained or archived in accordance with applicable law and/or by the order of a governmental or regulatory entity. Provided, however, that (i) such Personal Data shall be maintained for as long as such legal requirement applies; and (ii) The Personal Data that remains in the possession of Veego shall be subject to the same provisions of this DPA and shall be processed only as necessary for the purpose(s) specified in the applicable laws requiring its storage and for no other purpose.

10.2. Upon the Controller's prior written request, the Veego's Data Privacy Officer or equivalent shall provide written certification to the Controller that it has fully complied with this section.

10.3. The obligations under this Article 10 shall remain in force even after the termination of this DPA.

11. Provision of information.

Veego shall provide cooperation and assistance to the Controller, at the Controller's expense, with any data protection impact assessments, and prior consultations with relevant competent Data Privacy Authorities as required under Applicable Laws. The scope of such assistance shall be limited to the Processing of the Controller's Personal Data by Veego.

12. Audit rights.

12.1. Veego shall make available to the Controller, upon prior written request, not more than once a year, except in the event of a Personal Data Breach, information necessary to

demonstrate compliance with this DPA, including industry standard third-party audit certifications.

12.2. The Controller shall provide at least four (4) weeks prior written notice to Veego of a request to audit.

12.3. Veego shall allow for and contribute to audits, including inspections, by a reputable auditor mandated by the Controller, and agreed upon by Veego. Such reputable auditor shall be paid by the Controller. The scope, duration, and methods of such an audit will be determined by the Parties in good faith. In any event, a third-party auditor shall be subject to confidentiality obligations and a non-disclosure agreement. Veego may object to the selection of the auditor if it reasonably believes that an auditor does not guarantee confidentiality, security or otherwise puts at risk the Veego's business. The Controller shall avoid causing any damage, injury or disruption of Veego's premises, equipment, personnel, and business operations while performing the audit.

13. Cross-border data transfer.

13.1. Personal Data may be transferred from the country in which it originated to perform the Services for the Controller. The Controller shall obtain and maintain any and all necessary consents where applicable or ensure it has the right to allow for such transfer. Data transfers under the Agreement from the EEA, Switzerland and/or the United Kingdom to countries that do not offer an adequate level of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA, the European Union, Member States or the European Commission, without any further safeguard being necessary or otherwise under Applicable Laws or another official certification body to the extent permitted under Applicable Laws, shall be subject to the Standard Contractual Clauses attached in **Annex 4** ("**SCCs**").

13.2. Unless Veego transfers Personal Data according to 13.1, Veego shall execute and abide by the SCCs attached in **Annex 5**, which shall apply to the processing of Personal Data in countries outside the UK that do not provide the aforementioned adequate level of data protection.

13.3. Where and to the extent that the SCCs are applicable, if there is any conflict between this DPA and the SCCs, the SCCs shall prevail.

13.4. In any event, Veego shall provide the Controller with all relevant information to enable the Controller to comply with its obligations in case of cross-border transfers.

14. Term of the DPA.

The term of this DPA shall be the same as the term of the Agreement. Should any part of the Veego Services continue after the termination or expiration of the Agreement, then the provisions of this DPA shall continue to govern such services and for that purpose, this DPA shall remain in force and effect as long as such Veego Services are rendered by Veego.

15. Liability and indemnification.

15.1. The "*limitation of liability"* provisions as set forth in the certain Agreement **shall** apply to this DPA.

15.2. To the extent Veego shall be subject to any enforcement action or any third-party claim, based on any acts or omissions of the Controller relating to the end user's Personal Data, or any failure by the Controller to comply with any applicable Data Protection Laws, the Controller shall hold Veego harmless and fully indemnify Veego at its first demand, for any expenses, losses and damages, including without limitation, reasonable attorney's fees and

any fines and levies, incurred by Veego in connection with and as a result of such enforcement action or claim.

16. Miscellaneous.

16.1. Severance. If any provision or any part thereof contained in this DPA is, for any reason, held to be invalid, or unenforceable in any respect under the laws of any jurisdiction where enforcement is sought, such invalidity or unenforceability will not affect any other provision of this DPA and the remainder of the DPA will remain in force. The DPA will be construed as if such invalid or unenforceable provision or part thereof had never been contained therein, or shall be amended as needed to ensure its validity and enforceability.

16.2. Jurisdiction. This DPA shall be governed by and construed in accordance with the laws of the State of Israel. Any dispute arising out of or in connection with this DPA shall submit to the exclusive jurisdiction of the competent courts of Tel Aviv – Jaffa, Israel.

16.3. Notice. All notices required under this DPA shall be sent to each Party to the addresses as detailed in the Agreement.

16.4. Order of precedence. In the event of any conflict between the terms of this DPA and other documents binding on Parties, the terms of these documents will be interpreted according to the following order of precedence: (i) the SCCs (as applicable); (ii) this DPA; (iii) the Veego's Privacy Policy as published at the Veego's website; and (iv) terms of any agreement, license of subscription, scope of work (SOW), repursuant to which Veego's Services are provided.

IN WITNESS WHEREOF, this DPA is entered into and becomes binding between the Parties with effect from the date first set out above.

Annexes:

The following annexes are integral parts of this DPA:

Annex 1: List of parties; Description of transfer.

Annex 2: Technical and Organizational measures including technical and organizational measures to ensure the security of the data.

Annex 3: Sub Processors list

Annex 4: Standard Contractual Clauses - EU

Annex 5: Standard Contractual Clauses – UK

Annex 1

This **Annex 1** includes certain details of the Processing of Personal Data.

A. List of Parties

Data exporter(s):

1. Name: as detailed in the Agreement.
Address: as detailed in the Agreement.
Contact person's name, position and contact details: as detailed in the Agreement.
Signature and date: as detailed in the Agreement.
Role: Controller

Data importer(s):

1. Name: Veego Ltd.
Address: Ha'Yetsira St. 3, Ramat-Gan, Israel.
Contact person's name, position and contact details: Uri Fleyder-Kotler, CISO, uri@veego.io
Signature and date: as detailed in the Agreement.
Role: Processor

B. Description of transfer

1. *Categories of data subjects whose personal data is transferred*: The group of individuals affected by the processing of Personal Data under the Agreement may include the Controller's customers or Controller's users.

2. *Categories of personal data transferred*: The types of Personal Data that may be collected, processed and/or used under the Agreement may include the following: first and last names, domains, email addresses, company name, usernames, passwords, URLs, IPs, photos, MAC addresses, IMEIs, social network profiles, and documents. In the normal course of business, the Processor should not have access to any information other than encrypted data.

3. *Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures*: None.

4. *The frequency of the transfer*: On a continuous basis.

5. *Nature of the processing*: operations varies on the basis of the specific Service activated through the Agreement.

6. *Purpose(s) of the data transfer and further processing*: The data processing is for providing the requested services by Veego.

Annex 2 – Technical and Organizational measures

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

The Processor is compliant and will remain compliant throughout the terms of the Agreement and this DPA and therefore has implemented all the technical and organizational security requires measures.

Measures to ensure confidentiality:

1. Physical access control. Measures that physically deny authorized person access to IT systems and data processing equipment used to process Personal Data, as well as to confidential files and data storage media. Physical access control information is implemented according to the best practices.

2. Logical access control. Measures to prevent unauthorized persons from processing or using Personal Data that is protected by applicable privacy laws. Logical access control is implemented according to best practices.

3. Separation rule. Measures to ensure that Personal Data collected for different purposes are processed separately and separated from other data and systems in such a way as to unplanned use of such data for other purposes. Separation rule and separation control process implemented according to best practice.

4. Access Control: Veego enforce strict access controls to ensure that only authorized Veego Personnel can access Sensitive Personal Data. Veego achieve this through the use of strong passwords, Single Sign-On (SSO), VPN, two-factor authentication, and role-based access controls.

5. Security awareness training: Veego conduct annual security awareness training for all Veego employees to ensure that they understand their role in maintaining the company's security posture and can identify potential security threats.

Measures to ensure integrity:

1. Input control. Measures to ensure that it can be subsequently verified and ascertained whether and by whom Personal Data has been entered or modified in data processing systems. The Processor monitors access to its systems upon which Personal Data is processed and maintains logs of such access to its systems which shall include the following information: User identity, data and time of access attempt, system component to which access was attempted, access type, its scope, and whether access was granted or denied (the "Log Data"). The Log Data shall be retained by the Processor for at least 24 months and provided to the Controller upon request. The input control is implemented the according to best practices.

2. Encryption: Veego use AES 256-bit encryption to protects sensitive data both at rest and in transit.

3. Email security: MFA enforcement for all users, attachment protection, suspicious email link protection for IMAP users, external images and links protection, as well as domain spoofing and email authentication protection to combat phishing and malware threats.

4. Network security Veego have implemented firewalls, intrusion detection, Security Information and Event Management (SIEM), and other network security measures to protect against unauthorized access and network attacks.

5. Endpoint security: Veego protect its endpoints against malware, ransomware, and exploitation using a leading Endpoint Protection Platform (EPP) and Endpoint Detection and Response (EDR) solution. Veego ensure endpoint security posture (e.g., approves operations systems and versions, host firewall, security patches, disk encryption, password-protection, lock screen after inactivity period, etc.).

Measures to ensure availability and resilience.

1. Reliability. Measures to ensure that the functions of the system are available and implemented according to best practices.

2. Incident Response Plan: Veego have developed and implemented an incident response plan to ensure that security incidents are detected and responded to promptly and effectively.

Measures for the regular testing and evaluation of the security of data processing

1. Verification process. Measures to ensure that the data are processed securely and in compliance with data protection regulations. Such process is done via documentation of instructions received by the Controller. The Processor will conduct penetration testing of its systems every eighteen (18) months from the date of the Agreement. The Processor will perform a vulnerability and security assessment every eighteen (18) months from the date **of** the assessment, whether by its own qualified personnel or through a certified provider.

2. Order control. Measures to ensure that Personal Data processed on behalf of the Controller can only be processed in accordance with the instructions of the Controller.

3. Vulnerability Management: Veego perform continuous attack surface discovery, and scan our network, applications, source code, third-party dependencies, and contained images to identify and address any security issues.

Annex 3 – Sub-Processors' List

Entity	Location	Description	Purpose
Amazon Web Services (AWS)	USA	Cloud computing provider	Storing and processing data
Google Analytics	USA	Data analytics	Analyzing data
Hotjar	USA	Data analytics	Analyzing data
HubSpot	USA	CRM and marketing	Managing customer relationships, sending and receiving emails
Cloudflare	USA	Security provider	Securing data
Osano	USA	Compliance provider	Complying with laws and regulations

Annex 4 – Standard Contractual Clauses - EEA

Veego - EU SCCs.pdf

Annex 5 – Standard Contractual Clauses - UK

Table 1: Parties

As detailed in Annex 1 to this DPA, or as detailed in specific Agreement between the Parties.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or X the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2	X	X		General Authoriation	30	
3						
4						

Table 3 – appendix Information

All as attached as Annexes to this DPA.

Table 4 – Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter X neither Party