THIS DATA PROCESSING AGREEMENT

This DPA is entered into between the Data Controller and the Data Processor and is incorporated into and governed by the terms of the Agreement.

1 GENERAL

1.1 Any capitalised term not defined in this DPA shall have the meaning given to it in the Agreement:

Affiliate	Any entity that directly or indirectly controls, is controlled by, or is under common control of a party. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of a party.
Agreement	The agreement between the Data Controller and the Data Processor for the provision of the Services.
Client Data	Means all data imported into the Services for the purpose of using the Services or facilitating use of the Services by the Client or its users;
Data Controller	The Client named in the Agreement.
Data Processor	Datachoice Solutions Limited t/a Geckoboard, with company number 05958505 whose registered office is at 71-75 Shelton Street, Covent Garden, London WC2H 9JQ, United Kingdom, including any "Service Provider" as that term is defined in US State Privacy Laws.
Data Protection Legislation	All laws and regulations, including laws and regulations of the European Union, the European Economic Area, their member states and the United Kingdom any amendments, replacements or renewals thereof, applicable to the processing of Personal Data, including where applicable the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020, the EU GDPR, the UK GDPR, the FADP, the UK Data Protection Act 2018, US State Privacy Laws and any applicable national implementing

	laws, regulations and secondary legislation relating to the processing of Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time, including the Privacy and Electronic Communications Directive (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426).
DPA	This data processing agreement together with its exhibits.
Data Subject	Has the same meaning as in Data Protection Legislation or means a "Consumer" or (individual" as those terms are defined in US State Privacy Laws.
EEA	The European Economic Area.
EU GDPR	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, (General Data Protection Regulation).
FADP	The Swiss Federal Act on Data Protection of the 1st of September 2023, and as amended from time to time.
Personal Data	Has the same meaning as in Data Protection Legislation.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
Restricted Transfer	Means: (i) where the EU GDPR applies, a transfer of Personal Data via the Services from the EEA either directly or via onward transfer, to any country or recipient outside of the EEA not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of Personal Data via the Services from the United Kingdom either directly or via onward transfer, to any country or recipient outside of the UK not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) a transfer of Personal Data via the Services from Switzerland either directly or via onward transfer, to any country or recipient outside of the EEA and/or Switzerland not subject to an adequacy determination by the European Commission.
Services	All services and software applications and solutions provided to the Data Controller by the Data Processor under and as described in the Agreement.
Security Policy	The Data Processor's security document as updated from time to time set out in Exhibit 2 of this DPA.

Sub-Processor	Any third party (including Data Processor Affiliates) engaged directly by the Data Processor to process Personal Data under this DPA in the provision of the Services to the Data Controller.
SCCs	Means: (i) where the EU GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries published at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN/, ("**EU SCCs**"); and (ii) where the UK GDPR applies the international data transfer addendum to the EU SCCs adopted pursuant to Article 46(2)(c) of the UK GDPR and published at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf, as may be amended or replaced, ("**UK SCCs**"); and (iii) where Personal Data is transferred from Switzerland to outside of Switzerland or the EEA, the EU SCCs as amended in accordance with guidance from the Swiss Data Protection Authority; ("**Swiss SCCs**").
Supervisory Authority	A governmental or government chartered regulatory body having binding legal authority over a party.
UK GDPR	The EU GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018;
US State Data Protection Laws	The following US state data protection or privacy laws and regulations applicable to the party's Processing of Personal Data: California Consumer Privacy Act (**CCPA**) as amended by the California Privacy Rights Act (**CPRA**), Virginia Consumer Data Protection Act (**VCDPA**), Colorado Privacy Act (**CPA**), Connecticut Data Privacy Act (**CTDPA**), and Utah Consumer Privacy Act (**UCPA**) and the Connecticut Data Privacy Act (**CTDPA**), the Montana Consumer Data Privacy Act (**MCDPA**), Consumer Data Protection (**Iowa CDPA**), the Delaware Personal Data Privacy Act (**DPDPA**), the Nebraska Data Privacy Act (**NDPA**), the New Hampshire Expectation of Privacy Act (**NHPA**) and the New Jersey Act Concerning Online Services, Consumers, and Personal Data (**NJDPA**), in each case as may be amended or superseded from time to time.

1.2 Pursuant to and in consideration for the continued provision of the Services by the Data Processor for the benefit of the Data Controller the parties have entered into this DPA.

2 PURPOSE AND SCOPE

2.1 The Data Processor has agreed to provide the Services to the Data Controller in accordance with the terms of the Agreement. In providing the Services, the Data Processor shall process data provided by the Data Controller, on behalf of the Data Controller. Such data may include Personal Data. The Data Processor will process and protect such Personal Data in accordance with the terms of this DPA.

2.2 In providing the Services to the Data Controller pursuant to the terms of the Agreement, the Data Processor shall process Personal Data only to the extent necessary to provide the Services in accordance with the terms of the Agreement, this DPA and the Data Controller's instructions documented in the Agreement and this DPA, as updated from time to time.

2.3 The parties shall take steps to ensure that any natural person acting under the authority of the Data Controller or the Data Processor who has access to Personal Data does not process Personal Data except on the instructions from the Data Controller unless he or she is required to do so by any Data Protection Legislation.

3 DATA CONTROLLER'S OBLIGATIONS

3.1 To the extent that the Data Processor processes Personal Data in the course of providing the Services, each party acknowledges that, for the purposes of the Data Protection Legislation the Data Controller is the controller of any Personal Data.

3.2 The Data Controller represents and warrants that:

3.2.1 it shall comply with its obligations under this DPA and the Data Protection Legislation;

3.2.2 it has obtained any and all permissions and authorisations necessary to permit the Data Processor, its Affiliates and Sub-Processors, to execute their rights or perform their obligations under this DPA; and

3.2.3 all Affiliates of the Data Controller who use the Services shall comply with the obligations of the Data Controller set out in this DPA.

3.3 The Data Controller shall implement appropriate technical and organisational measures to protect Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The Data Controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

3.3.1 The pseudonymisation and encryption of Personal Data;

3.3.2 The ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services;

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

3.3.4 A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In accessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

3.4 The Data Controller acknowledges and agrees that some instructions from the Data Controller, including the Data Processor assisting with audits, inspections, DPIAs or providing any assistance under this DPA, may result in additional fees. The Data Processor shall be entitled to charge the Data Controller for its costs and expenses in providing any such assistance.

4 DATA PROCESSOR'S OBLIGATIONS

4.1 To the extent that the Data Processor processes Personal Data in the course of providing the Services, each party acknowledges that, for the purposes of the Data Protection Legislation the Data Processor is the processor of any Personal Data.

4.2 The Data Processor may collect, process or use Personal Data only within the scope of this DPA.

4.3 The Data Processor confirms that it shall process Personal Data on behalf of the Data Controller in accordance with the documented instructions of the Data Controller.

4.4 The Data Processor shall promptly inform the Data Controller, if in the Data Processor's opinion, any of the instructions regarding the processing of Personal Data provided by the Data Controller, breach any Data Protection Legislation.

4.5 The Data Processor shall ensure that all employees, agents, officers and contractors involved in the handling of Personal Data:

4.5.1 Are aware of the confidential nature of the Personal Data and are contractually bound to keep the Personal Data confidential;

4.5.2 Have received appropriate training on their responsibilities as a data processor; and

4.5.3 Are bound by the terms of this DPA.

4.5.4 The Data Processor shall implement appropriate technical and organisational measures to protect Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

4.6 The Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

4.6.1 the pseudonymisation and encryption of Personal Data;

4.6.2 the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services;

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

4.6.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In accessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

4.7 The technical and organisational measures detailed in the Security Policy shall at all times be adhered to as a minimum security standard. The Data Controller accepts and agrees that the technical and organisational measures are subject to development and review and that the Data Processor may use alternative suitable measures to those detailed in the attachments to

this DPA, provided such measures are at least equivalent to the technical and organisational measures set out in the Security Policy and appropriate pursuant to the Data Processor's obligations in clauses 4.5 and 4.6 above.

4.8 Taking into account the nature of the processing and the information available to the Data Processor, the Data Processor shall assist the Data Controller by having in place appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the Data Subject's rights and the Data Controller's compliance with the Data Controller's data protection obligations in respect of the processing of Personal Data.

4.9 The Data Processor may not:

4.9.1 Sell Personal Data;

4.9.2 Retain, use, or disclose Personal Data for commercial purposes other than providing the Services under the terms of the Agreement; or

4.9.3 Retain, use, or disclose Personal Data outside of the Agreement.

5 DATA SUBJECT ACCESS REQUESTS

5.1 The Data Processor shall:

5.1.1 taking into account the nature of the processing and the information available to the Data Processor, assist the Data Controller by having in place appropriate technical and organisational measures, in so far as this is possible, for the fulfilment of the Data Controller's obligation to respond to requests by Data Subjects to exercise their rights of access, rectification or erasure, to restrict or object to processing of Personal Data, or to data portability; and

5.1.2 if a Data Subject makes a request to the Data Processor to exercise any of the rights referred to in clause forward the request to the Data Controller promptly and shall, upon the Data Controller's reasonable written request, provide the Data Controller with all co-operation and assistance reasonably requested by the Data Controller in relation to that request to enable the Data Controller to respond to that request in compliance with applicable deadlines and information requirements. The Data Controller shall reimburse the Data Processor for all costs incurred resulting from providing assistance in dealing with a Data Subject request. In the event that the Data Processor is legally required to respond to the Data Subject, the Data Controller will fully cooperate with the Data Processor as applicable.

6 PERSONAL DATA BREACH

6.1 The Data Processor shall notify the Data Controller without undue delay after becoming aware of a Personal Data Breach (and in any event within 72 hours of discovering a Personal Data Breach).

6.2 The Data Processor shall take all commercially reasonable measures to secure the Personal Data, to limit the effects of any Personal Data Breach, and to assist the Data Controller in meeting the Data Controller's obligations under applicable law.

7 SUB-PROCESSORS

7.1 The Data Controller acknowledges and agrees that the Data Processor may engage Sub-Processors in connection with the provision of the Services.

7.2 All Sub-Processors who process Personal Data in the provision of the Services to the Data Controller shall comply with the obligations of the Data Processor set out in this DPA.

7.3 The Data Controller authorises the Data Processor to use the Sub-Processors included in the list of Sub-Processors accessible via: https://www.geckoboard.com/legal/subprocessors/ to process the Personal Data. During the term of this DPA, the Data Processor shall provide the Data Controller with 30 days prior notification, via email, of any changes to the list of Sub-Processors before authorising any new or replacement Sub-Processor to process Personal Data in connection with provision of the Services.

7.4 The Data Controller may object to the use of a new or replacement Sub-Processor, by notifying the Data Processor promptly in writing within 14 days after receipt of the Data Processor's notice. If the Data Controller objects to a new or replacement Sub-Processor, the Data Controller may terminate the Agreement with respect to those Services which cannot be provided by the Data Processor without the use of the new or replacement Sub-Processor.

7.5 All Sub-Processors who process Personal Data shall comply with the obligations of the Data Processor set out in this DPA. The Data Processor shall prior to the relevant Sub-Processor carrying out any processing activities in respect of the Personal Data:

7.5.1 Appoint each Sub-Processor under a written contract containing materially the same obligations to those of the Data Processor in this DPA enforceable by the Data Processor; and

7.5.2 Ensure each such Sub-Processor complies with all such obligations.

7.6 The Data Controller agrees that the Processor and its Sub-Processors may make Restricted Transfers of Personal Data for the purpose of providing the Services to the Data Controller in accordance with the Agreement. The Data Processor confirms that such Sub-Processors:

7.6.1 Are located in a third country or territory recognised by the EU Commission or a Supervisory Authority, as applicable, to have an adequate level of protection; or

7.6.2 Have entered into the applicable SCCs with the Data Processor; or

7.6.3 Have other legally recognised appropriate safeguards in place.

8 RESTRICTED TRANSFERS

8.1 The parties agree that, when a transfer of Personal Data occurs between the Data Controller and the Data Processor or from the Data Processor to a Sub-Processor which is a Restricted Transfer, it shall be subject to the applicable SCCs.

8.2 The parties agree that the EU SCCs shall apply to Restricted Transfers from the EEA. The EU SCCs shall be deemed entered into (and incorporated into this DPA by reference) and completed as follows:

8.2.1 Module Two (Controller to Processor) shall apply where the Client is a Data Controller of Personal Data and Geckoboard is processing Personal Data;

8.2.2 Module Three (Processor to Processor) shall apply where Geckoboard is a Data Processor of Personal Data and Geckoboard uses a Sub-Processor to process the Personal Data;

8.2.3 Module Four (Processor to Controller) shall apply where Geckoboard id processing Personal Data and the Client is not subject to the EU GDPR or UK GDPR;

8.2.4 In Clause 7 of the EU SCCs, the optional docking clause shall not apply;

8.2.5 In Clause 9 of the EU SCCs Option 2 applies, and the time period for giving notice of Sub-Processor changes shall be as set out in clause 7.3 of this DPA;

8.2.6 In Clause 11 of the EU SCCs, the optional language shall not apply;

8.2.7 In Clause 17 of the EU SCCs, Option 1 applies and the EU SCCs shall be governed by Austrian law;

8.2.8 In Clause 18(b) of the EU SCCs, disputes shall be resolved by the courts of Austria;

8.2.9 Annex I of the EU SCCs shall be deemed completed with the information set out in Exhibit 1 of this DPA;

8.2.10 Annex II of the EU SCCs shall be deemed completed with the information set out in Exhibit 2 of this DPA.

8.3 The parties agree that the EU SCCs as amended in clause 8.2 above, shall be adjusted as set out below where the FADP applies to any Restricted Transfer:

8.3.1 The Swiss Federal Data Protection and Information Commissioner ("**FDPIC**") shall be the sole Supervisory Authority for Restricted Transfers exclusively subject to the FADP;

8.3.2 Restricted Transfers subject to both the FADP and the EU GDPR, shall be dealt with by the EU Supervisory Authority named in Exhibit 1 of this DPA;

8.3.3 The term 'member state' must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs;

8.3.4 Where Restricted Transfers are exclusively subject to the FADP, all references to the GDPR in the EU SCCs are to be understood to be references to the FADP;

8.3.5 Where Restricted Transfers are subject to both the FADP and the EU GDPR, all references to the GDPR in the EU SCCs are to be understood to be references to the FADP insofar as the Restricted Transfers are subject to the FADP;

8.4 The parties agree that the UK SCCs shall apply to Restricted Transfers from the UK and the UK SCCs shall be deemed entered into (and incorporated into this DPA by reference), completed as follows:

8.4.1 Table 1 of the UK SCCs shall be deemed completed with the information set out in Exhibit 1 of this DPA;

8.4.2 Table 2 of the UK SCCS shall be deemed completed with the information set out in clauses 8.2.1 – 8.2.8 of this DPA;

8.4.3 Table 3 of the UK SCCs shall be deemed completed with the information set out in

Exhibits 1 and 2 of this DPA; and

8.4.4 Either party may end the UK SCCs as set out in clause 19 of the UK SCCs.

8.5 If changes are made to the EU SCCs or UK SCCs in the future, the parties shall negotiate in good faith necessary amendments to the DPA and the Agreement to ensure compliance with applicable Data Protection Legislation.

8.6 In the event that any provision of this DPA contradicts directly or indirectly any SCCs, the provisions of the applicable SCCs shall prevail over the terms of the DPA.

8.7 Should countries other than those in the EEA, UK or Switzerland adopt cross-border data transfer clauses similar to the SCCs, the Controller and Processor agree to execute such clauses when necessary.

9 COMPLIANCE, COOPERATION AND RESPONSE

9.1 The Data Processor shall maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless the Data Controller or this DPA specifically authorises the disclosure, or as required by law. If a law, court, regulator or Supervisory Authority requires the Data Processor to process or disclose Personal Data, the Data Processor must first inform the Data Controller of the legal or regulatory requirement and give the Data Controller an opportunity to object or challenge the requirement, unless the law prohibits giving such notice.

9.2 The Data Processor may make copies of and/or retain Personal Data in compliance with any legal or regulatory requirements including, but not limited to, retention requirements.

9.3 The Data Processor shall notify the Data Controller promptly if it receives any complaint, notice or communication which relates:

9.3.1 directly to the processing of Personal Data which adversely impacts the Data Controller; or

9.3.2 to either party's compliance with Data Protection Legislation;

unless such notification is not permitted under applicable law or a relevant court order and shall fully co- operate and assist the Data Controller in relation to any such complaint, notice, communication or non-compliance.

9.4 The Data Controller and the Data Processor and, where applicable, their representatives, shall cooperate, on request, with a Supervisory Authority in the performance of their respective obligations under this DPA and Data Protection Legislation.

9.5 The Data Processor shall reasonably assist the Data Controller in meeting the Data Controller's obligation to carry out data protection impact assessments (DPIAs), taking into account the nature of the processing and the information available to the Data Processor.

9.6 The Data Controller shall notify the Data Processor within a reasonable time, of any changes to applicable data protection laws, codes or regulations which may affect the contractual duties of the Data Processor. The Data Processor shall respond within a reasonable timeframe in respect of any changes that need to be made to the terms of this DPA or to the technical and organisational measures to maintain compliance. If the parties agree that amendments are required, but the Data Processor is unable to accommodate the necessary changes, the Data Controller may terminate the part or parts of the Services which give rise to the non-compliance. To the extent that other parts of the Services provided are not affected by such

changes, the provision of those Services shall remain unaffected.

10 AUDIT

10.1 The Data Processor shall make available to the Data Controller all information reasonably necessary to demonstrate compliance with its processing obligations and allow for and contribute to audits and inspections.

10.2 Any audit conducted under this DPA shall consist of examination of the most recent reports, certificates and/or extracts prepared by an independent auditor bound by confidentiality provisions similar to those set out in the Agreement. In the event that provision of the same is not deemed sufficient in the reasonable opinion of the Data Controller, the Data Controller may conduct a more extensive audit which will be:

10.2.1 At the Data Controller's expense, which shall include all costs and expenses incurred by the Data Processor;

10.2.2 Limited in scope to matters specific to the Data Controller and agreed in advance;

10.2.3 Carried out during the Data Processor's usual business hours and upon reasonable notice which shall be not less than 4 weeks unless an identifiable material issue has arisen; and

10.2.4 Conducted in a way which does not interfere with the Data Processor's day-to-day business.

10.3 This clause shall not modify or limit the rights of audit of the Data Controller, instead it is intended to clarify the procedures in respect of any audit undertaken pursuant thereto.

11 LIABILITY

11.1 The limitations on liability set out in the Agreement apply to all claims made pursuant to any breach of the terms of this DPA.

11.2 The parties agree that the Data Processor shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Sub-Processors to the same extent the Data Processor would be liable if performing the services of each Sub-Processor directly under the terms of the DPA, subject to any limitations on liability set out in the terms of the Agreement.

11.3 The parties agree that the Data Controller shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Affiliates as if such acts, omissions or negligence had been committed by the Data Controller itself.

11.4 The Data Controller shall not be entitled to recover more than once in respect of the same loss.

12 TERM, TERMINATION AND EXPIRY

12.1 This DPA will remain in full force and effect so long as the Data Processor continues to provide the Services to the Data Controller under the Agreement, or the Data Processor retains any Personal Data that is the subject of the DPA in its possession or control.

13 DELETION AND RETURN OF PERSONAL DATA

13.1 The Data Processor shall, at the Data Controller's option, upon receipt of a written request received within 30 days of the end of the provision of the Services, return the Personal Data to the Data Controller or to a processor nominated by the Data Controller or delete the Personal Data within 12 months of the effective date of termination of the Agreement, including all copies and extracts of the Personal Data unless, applicable law or regulations require storage of the Personal Data after termination.

13.2 On expiry or termination (however arising) the terms of this DPA shall survive and continue in full force and effect.

14 MISCELLANEOUS PROVISIONS

14.1 This DPA sets out the entire understanding of the parties with regard to the subject matter herein.

14.2 Should a provision of this DPA be invalid or become invalid then the legal effect of the other provisions shall be unaffected. A valid provision is deemed to have been agreed which comes closest to what the parties intended commercially and shall replace the invalid provision. The same shall apply to any omissions.

14.3 Subject to any provision of the SCCs to the contrary, this DPA and any non-contractual obligations arising out of or in connection with it are governed by English law and the courts of England have exclusive jurisdiction to settle any dispute arising out of or in connection with this DPA and the parties submit to the exclusive jurisdiction of the English courts.

14.4 The parties agree that this DPA is incorporated into and governed by the terms of the Agreement.

EXHIBIT 1

List of Parties, Description of Processing and Transfer of Personal Data, Competent Supervisory Authority

A. LIST OF PARTIES

The Exporter:

means the Client.	
Address:	As set out for the Client in the Agreement.
Contact person's name, position and contact details:	As provided by the Client in its account and used for notification and invoicing purposes.
Activities relevant to the data transferred under the SCCs:	Use of the Services.
Signature and date:	By entering into the Agreement, the Exporter is deemed to have signed the SCCs incorporated into this DPA and including their Annexes, as of the Effective Date of the Agreement.
Role:	Data Controller.
Name of Representative (if applicable):	Any UK or EU representative named in the Exporter's privacy policy.

The Importer:

means Datachoice Solutions Limited t/a Geckoboard	
Address:	71-75 Shelton Street, Covent Garden, London, WC2H 9JQ, United Kingdom.
Contact person's name, position and contact details:	Luis Hernandez, Head of Data Privacy, privacy@geckoboard.com
Activities relevant to the data transferred under the SCCs:	The provision of cloud computing solutions to the Exporter under which the Importer processes Personal Data upon the instructions of the Exporter in accordance with the terms of the Agreement.
Signature and date:	By entering into the Agreement, the Importer is deemed to have signed the SCCs, incorporated into this DPA, including their Annexes, as of the Effective Date of the Agreement.
Role:	Data Processor.

Name of Representative (if applicable):	GDPR-Rep.eu of Schellinggasse 3/10, 1010 Vienna, Austria contact@gdpr-rep.eu

B. DESCRIPTION OF PROCESSING AND TRANSFERS

Categories of Data Subjects:	Employees, agents, advisors, consultants, freelancers of the Data Controller (who are natural persons). Users, Affiliates and other participants authorised by the Data Controller to access or use the Services in accordance with the terms of the Agreement. Prospects, customers, clients, business partners and vendors of the Data Controller (who are natural persons) and individuals with whom those end users communicate with by email and/or other messaging media. Employees or contact persons of Data Controller's prospects, customers, clients, business partners and vendors. Suppliers and service providers of the Data Controller. Other individuals to the extent identifiable in the context of emails of their attachments or in archiving content.
Categories of Personal Data:	The Data Controller may submit Personal Data to the Services, the extent of which is determined and controlled by the Data Controller. The Personal Data includes but is not limited to: • Personal details, names, email addresses of users of the Services. • Content of live chat and email communications. • Unique identifiers such as username, account number or password. • Personal Data derived from a user's use of the Services such as records and business intelligence information. • Personal Data within email and messaging content which identifies or may reasonably be used to identify, Data Subjects. • Meta data including sent, to, from, date, time, subject, which may include Personal Data. • Geolocation based upon IP address. • Financial data required for invoicing.

	• File attachments that may contain Personal Data • Information offered by users as part of support enquiries • Information about website and application browsing, and device information • Other data added by the Data Controller from time to time
Sensitive Data:	No sensitive data will be processed or transferred and shall not be contained in the content of or attachments to, emails.
The frequency of the processing and transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous basis for the duration of the Agreement.
Nature of the processing:	Personal Data will be processed during the course of providing the Services pursuant to the Agreement which may include operation of a cloud-based customer services platform. The Data Processor will process Personal Data in accordance with the Data Controller's instructions.
Purpose(s) of the data transfer and further processing:	Personal Data is transferred to sub-contractors who need to process some of the Personal Data in order to provide their services to the Data Processor as part of the Services provided by the Data Processor to the Data Controller.
The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:	Unless agreed otherwise in writing, for 12 months after the Agreement has been terminated.
For transfers to (Sub-) processors, also specify subject matter, nature and duration of the processing:	The Sub-Processor list accessed via https://www.geckoboard.com/legal/subprocessors/sets out the Personal Data processed by each Sub-Processor and the services provided by each Sub-Processor.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies (e.g. in accordance with Clause 13 of the SCCs)	Where the EU GDPR applies, Austrian Data Protection Authority – Österreichische Datenschutzbehörde (dsb). Where the UK GDPR applies, the UK Information Commissioner's Office, (ICO). Where the FADP applies, the Swiss Federal Data Protection and Information Commissioner, (FDPIC).

EXHIBIT 2

Technical and Organisational Security Measures (Including Technical and Organisational Measures to Ensure the Security of Data)

Below is a description of the technical and organisational measures implemented by the Data Processor 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.

Full details of the Data Processor's technical and organisational security measures used to protect Personal Data is available at https://support.geckoboard.com/hc/en-us/articles/203759278-Geckoboard-Security

Where applicable this Exhibit 2 will serve as Annex II to the SCCs.

Measure	Description
Measures of pseudonymisation and encryption of Personal Data	All communication between the Data Controller and the Data Processor is encrypted using HTTPS (256-bit TLS). This is the same level of encryption used by banks and financial institutions and is designed to prevent third parties from seeing information sent to or receiving from the Data Processor. Encryption technology is used to protect data stored on all databases, backup media, laptops, etc. Data Controller's data in both live and backup environments is encrypted at rest. Data Controller's credentials for third party services are encrypted with aes256-gcm96
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Access to data necessary for the performance of the particular task is ensured within the systems and applications by a corresponding role and authorisation concept. In accordance with the "least privilege" and "need-to-know" principles, each role has only those rights which are necessary for the fulfilment of the task to be performed by the individual person. Machines within the Data Processor's infrastructure are protected from the ground up. Data Processor uses Amazon Web Services (AWS) for hosting. AWS is an industry leader and provides a highly scalable cloud computing platform with end-to-end security and privacy features built in. All servers are provisioned with the minimum set of apps and services required to perform their function. Data Processor's employees do not have physical access to the servers in AWS. Electronic access to AWS servers and services

	is restricted to a core set of approved Data Processor's staff only. Remote access is available (i.e. for system maintenance), communication is encrypted and access authenticated by VPN. Devices not managed and affiliated to Data Processor are unable to remote into our internal network via VPN. To maintain data access control, state of the art encryption technology is applied to the Personal Data itself where deemed appropriate to protect sensitive data based on risk.
Measures for ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident	All of the Data Processor's applications are built stateless by using Cloud-formation templates and can be easily recreated. The data centres can be switched in the event of flooding, earthquake, fire or other physical destruction or power outage protect Personal Data against accidental destruction and loss. The Data Processor maintains redundancy throughout its IT infrastructure in order to minimize the lack of availability to or loss of data. Backups are maintained in accordance with our backup procedures. Data Processor's Ops team operates like a NOC to actively monitor the performance of the application 24 hours a day. The team is responsible for the security of the platform and are responsible for all software updates. Data Processor continuously reviews risks to application and business data. Internal policies have been designed to address risks.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	Data Processor's monitoring is automated and runs 24/7. These automated systems will alert the Data Processor's Ops team to any issues during business hours or on-call engineers out of hours Security updates are installed every night, or sooner for more serous vulnerabilities Data Processor undertakes PCI scanning on a regular basis and penetration testing on an annual basis. Additionally, Data Processor runs a public bug bounty program that rewards researchers for responsibly disclosing security vulnerabilities.
Measures for user identification and authorisation	All remote SSH access to Data Processor's infrastructure is only permitted via bastion host and is restricted to using pre-approved RSA2048-bit key pairs with no password authentication or root login. Furthermore, superuser access is restricted to trusted administrators only.

Measures for the protection of data during transmission	Data in transit is protected by Transport Layer Security ("TLS").
Measures for the protection of data during storage	Personal Data is only retained internally, and on the third party data centre servers, which are covered by AWS certifications. No customer data is stored on Data Processor's employee laptops where log-out after a fixed period of inactivity is enforced. The Data Controller's archived data is encrypted at rest using AES256 bit encryption and data in transit is protected by Transport Layer Security ("TLS"). The encryption keys for Data Processor's databases are managed by AWS' KMS service, which uses Hardware Security Modules (HSMs) to protect the security of the keys. Data Processor also uses HashiCorp's Vault to encrypt sensitive data. Access to those keys is restricted to members of Data Processor's Ops team.
Measures for ensuring physical security of locations at which Personal Data are processed	Physical access to Data Processor's office is tightly controlled. Office is protected by 24-hour security, CCTV and a keycard-based entry system. All maintenance personnel are supervised whilst onsite. Access to AWS data centres is strictly controlled and monitored using a variety of physical controls, intrusion detection systems, environmental security measures, 24 x 7 on-site security staff, biometric scanning, multi-factor authentications, video surveillance and other electronic means. All physical and electronic access to data centres by Amazon employees is authorized strictly on a least privileged basis and is logged and audited routinely. The AWS security provisions will apply as set out at https://aws.amazon.com/compliance/data-center/controls/. Data Processor's employees do not have physical access to servers in AWS. Electronic access to AWS servers and services is restricted to a core set of approved Data Processor's staff only.
Measures for ensuring events logging	Data Processor has system audit and event logging in place although alerts are generally generated based on collected metrics instead as this allows alerting on specific service-impacting criteria. Logs are generated when new releases are deployed, which are aggregated in CloudWatch in order to help developers troubleshoot any issues around a deployment.

	Administrator actions for support purposes are audit-logged and kept permanently.
Measures for ensuring system configuration, including default configuration	The Data Processor uses configuration management tools to deploy and enforce baseline configurations on their systems.
Measures for internal IT and IT security governance and management	Employees are instructed to collect, process and use Personal Data only within the framework and for the purposes of their duties (e.g. service provision). At a technical level, multi-client capability includes separation of functions as well as appropriate separation of testing and production systems. The Data Controller's Personal Data is stored in a way that logically separates it from other customer data.
Measures for certification/assurance of processes and products	The Data Processor utilizes Amazon Web Services (AWS) data centres. AWS is an industry leader and provides a highly scalable cloud computing platform with end-to-end security and privacy features built in and maintain ISO 27001, PCI-DSS, SOC 1, and SOC 2 certifications. The Data Processor will only use third party data centres that maintain the aforementioned certifications and/or attestations, or that have other substantially similar or equivalent certifications and/or attestations. See: https://aws.amazon.com/compliance/iso-certified/
Measures for ensuring data minimisation	If Personal Data is no longer required for the purposes for which it was processed, it is deleted promptly. It should be noted that with each deletion, the Personal Data is only locked in the first instance and is then deleted for good with a certain delay. This is done in order to prevent accidental deletions or possible intentional damage.
Measures for ensuring data quality	All of the data processed is provided by the Data Controller. The Data Processor does not assess the quality of the data provided by the Data Controller.
Measures for ensuring limited data retention	The Data Processor uses a data classification scheme for all data that it stores. When a record with Personal Data is deleted then it will be permanently removed from the Processor's active databases. The data is retained in backups for 14 days.
Measures for ensuring accountability	The Data Processor internally reviews its information security policies semi-annually to ensure they are still relevant and are being followed. All employees that handle sensitive data must acknowledge the information security policies. These employees are re-trained on information security policies once

	per year. A disciplinary policy is in place for employees that do not adhere to information security policies.
Measures for allowing data portability and ensuring erasure	The Services have built-in tools that allow the Data Controller to export and permanently erase data. The Data Processor provides an API which can be accessed by the users of an account. This API allows, create, read, update and delete actions on the main account data. API access levels are the same as the user would have within the web-app.
Measures to be taken by the (Sub-)Processor to be able to provide assistance to the Controller (and, for transfers from a Processor to a Sub-Processor, to the Data Exporter).	The transfer of Personal Data to a third party (e.g. customers, sub-contractors, service providers) is only made if a corresponding contract exists, and only for the specific purposes. If Personal Data is transferred outside the EEA, the Data Processor provides that an adequate level of data protection exists at the target location or organisation in accordance with the European Union's data protection requirements, e.g. by employing contracts based on the EU SCCs.