Customer Data Processing Addendum

This Data Processing Addendum **(“DPA”)** forms an integral part of the Agreement (“Main Agreement”) between Frontegg Ltd. **("Company")** and between the counterparty agreeing to these terms **("Customer";** each **“Party”** and together **“Parties”)** and applies to the extent that Company processes Personal Data on behalf of the Customer, in the course of its performance of its obligations under the Main Agreement.

If you are accepting this DPA on behalf of Customer, you warrant that: (a) you have full legal authority to bind Customer to this DPA; (b) you have read and understand this DPA; and (c) you agree, on behalf of Customer, to this DPA. If you do not have the legal authority to bind Customer, please do not accept this DPA.

All capitalized terms not defined herein shall have the meaning set forth in the Main Agreement.

1. Definitions

1.1 **"Approved Jurisdiction"** means a member state of the European Economic Area, or other jurisdiction as may be approved as having adequate legal protections for data by the European Commission currently found here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protecti on/adequacy-decisions_en.

1.2 **"Data Protection Law"** means, as applicable, any and/or all applicable domestic and foreign laws, rules, directives and regulations, on any local, provincial, state or federal or national level, pertaining to data privacy, data security and/or the protection of Personal Data, including the Privacy and Electronic Communications Directive 2002/58/EC (and respective local implementing laws) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), including any amendments or replacements to them, including the 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 **(“GDPR”),** including the Data Protection Act 2018 and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th 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) 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 **("UK GDPR")** and including the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. **("CCPA"),** and any amendment or successor law thereto, including the California Privacy Rights Act **(“CPRA”).**

1.3 **“Data Subject”** means an individual to whom Personal Data relates. Where applicable, Data Subject shall be deemed as a **"Consumer"** as this term is defined under the CCPA.

1.4 **"EEA"** means those countries that are member of the European Economic Area.

1.5 **“Permitted Purposes”** mean any purposes in connection with Company performing its obligations under the Main Agreement.

1.6 "Security Incident" shall mean any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed. For the avoidance of doubt, any Personal Data Breach (as defined under the GDPR) will comprise a Security Incident.

1.7 **“Security Measures”** mean commercially reasonable security-related policies, standards, and practices commensurate with the size and complexity of Company's business, the level of sensitivity of the data collected, handled and stored, and the nature of Company's business activities.

1.8 **"Standard Contractual Clauses"** mean the applicable module of the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council from 4 June 2021 as available here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en .

1.9 **"UK Standard Contractual Clauses"** mean the Standard Contractual Clauses in the following amendments: (1) The supervisory authority shall be the Information Commissioner's Office; (2) The Parties choose the English courts as their choice of forum and jurisdiction; (3) References to the “Union”, “EU” and “EU Member State” are all replaced with the “UK”; (4) The laws of England and Wales shall govern the UK Standard Contractual terms.

1.10 **“Sub-Processor(s)”** mean any Affiliate, agent or assignee of Company that may process Personal Data pursuant to the terms of the Main Agreement, and any unaffiliated processor, vendors or service provider engaged by Company.

1.11 The terms **"Business", “Controller”, "Personal Data", “Processor”, “Process”, “Processing”** and **"Service Provider"** shall have the meanings ascribed to them in the Data Protection Law, as applicable.

2. Application of this DPA

2.1 This DPA will only apply to the extent all of the following conditions are met:

(A) Company processes Personal Data that is made available by the Customer in connection with the Main Agreement (whether directly by the Customer or indirectly by a third party retained by and operating for the benefit of the Customer);

(B) The Data Protection Law apply to the processing of Personal Data.

2.2 This DPA will only apply to the services for which the Parties agreed to in the Main Agreement **("Services"),** which incorporates the DPA by reference.

3. Parties' Role

3.1 In respect of the Parties' rightsand obligations under this DPA regarding the Personal Data, the Parties hereby acknowledge and agree that the Customer is the Controller or Processor (as well as, as applicable, the Business or Service Provider, as these terms are defined under the CCPA) and Company is a Processor or Sub-Processor (as well as, as applicable, the Service Provider, as this term is defined under the CCPA), and accordingly:

(A) Company agrees that it shall process all Personal Data in accordance with its obligations pursuant to this DPA and Data Protection Law;

(B) The Parties acknowledge that the Customer discloses Personal Data to Company only for the performance of the Services and that this constitutes a valid business purpose for the processing of such data.

3.2 If Customer is a Processor, Customer warrants to Company that Customer's instructions and actions with respect to the Personal Data, including its appointment of Company as another Processor and concluding the Standard Contractual Clauses, have been authorized by the relevant controller.

3.3 Notwithstanding anything to the contrary in the DPA, Customer acknowledges that Company shall have the right to collect, use and disclose data:

(A) Collected in the context of providing the Services, for the purpose of the operation, support or use of its services for its legitimate business purposes, such as account management, technical support, troubleshooting, security, protecting against fraudulent or illegal activity, billing, and for the purpose of establishment/exercise and defense of legal claims.

(B) (Collected in the context of using the Services, for the purpose of analytics, market research, product improvement and development, provided however that the foregoing shall be based solely on the processing of aggregated and/or anonymized

(C) information.

(D) Collected directly from any individuals in the context of surveys, interviews, testing or research activities, for the purpose of product improvement and/or development (including any feedback).

Collected from the Customer's authorized representatives (e.g. employees) and/or authorized users, strictly for the purpose of administrating the business and/or contractual relationship with the Customer, including for billing, audit and recordkeeping purposes.

3.4 To the extent that any data referred under section 3.3 is considered as Personal Data, then Company shall be regarded as an independent Controller of such data under the Data Protection Law. In such case, Company shall process Personal Data in accordance with its obligations under Data Protection Law.

4. Compliance with Laws

4.1 Each Party shall comply with its respective obligations under the Data Protection Law.

4.2 Company shall provide reasonable cooperation and assistance to Customer in relation to Company's processing of Personal Data in order to allow Customer to comply with its obligations as a Data Controller under the Data Protection Law or its contractual obligations as a Processor.

4.3 Company agrees to notify Customer promptly if it becomes unable to comply with the terms of this DPA or Data Protection Law and take reasonable and appropriate measures to remedy such non-compliance.

4.4 Throughout the duration of the DPA, Customer agrees and warrants that:

(A) Personal Data has been and will continue to be collected, processed and transferred by Customer in accordance with the relevant provisions of the Data Protection Law;

(B) Where it serves as a Controller, Customer is solely responsible for determining the lawfulness of the data processing instructions it provides to Company and shall provide Company only instructions that are lawful under Data Protection Law;

(C) the processing of Personal Data by Company for the Permitted Purposes, as well as any instructions to Company in connection with the processing of the Personal Data ("Processing Instructions"), has been and will continue to be carried out in accordance with the relevant provisions of the Data Protection Law; and that

(D) The Customer will inform, or, where applicable, require the Controller to inform, Data Subjects of the processing and transfer of Personal Data pursuant to the DPA and obtained the relevant consents or lawful grounds thereto (including without limitation any consent required in order to comply with the Processing Instructions and the Permitted Purposes).

5. Processing Purpose and Instruction

5.1 The subject matter of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, shall be as set out in the Agreement, or in the attached Annex 1, which is incorporated herein by reference.

5.2 Company shall process Personal Data only for the Permitted Purposesand in accordance with Customer's written Processing Instructions, the

Agreement and the Data Protection Law, unless Company is otherwise required to do so by law to which it is subject (and in such a case, Company shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest).

5.3 To the extent that any Processing Instructions may result in the Processing of any Personal Data outside the scope of the Agreement and/or the Permitted Purposes, then such Processing will require prior written agreement between Company and Customer, which may include any additional fees that may be payable by Customer to Company for carrying out such Processing Instructions. Company shall immediately inform Customer if, in Company's opinion, an instruction is in violation of Data Protection Law.

5.4 Additional instructions of the Customer outside the scope of the Agreement require prior and separate agreement between Customer and Company, including agreement on additional fees (if any) payable to Company for executing such instructions.

5.5 Company shall not sell, retain, use or disclose the Personal Data for any purpose other than for the specific purpose of performing the Services or outside of the direct business relationship between the Parties, including for a commercial purpose other than providing the Services, except as required under applicable laws, or as otherwise permitted under the CCPA (if applicable) or as may otherwise be permitted for service providers or under a comparable exemption from "sale" in the CCPA (as applicable), as reasonably determined by Company. Company's performance of the Services may include disclosing Personal Data to Sub-Processors where this is relevant in accordance with this DPA. The Company certifies that it, and any person receiving access to Personal Data on its behalf, understand the restrictions contained herein

6. Reasonable Security and Safeguards

6.1 Company represents, warrants, and agrees to use Security Measures (i) to protect the availability, confidentiality, and integrity of any Personal Data collected, accessed or
processed by Company in connection with this Agreement, and (ii) to protect such data from Security Incidents.

6.2 The Security Measures are subject to technical progress and development and Company may
update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the services procured by Customer.

6.3 Company shall take reasonable steps to ensure the reliability of its staff and any other person acting under its supervision who has access to and processes Personal Data. Company shall ensure that persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6.4 Company is responsible for performing its obligations under the Agreement in a manner which enables Company to comply with Data Protection Law, including implementing appropriate technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the processing of Personal Data, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

7. Security Incidents

7.1 Upon becoming aware of a Security Incident, Company will notify Customer without undue delay and will provide information relating to the Security Incident as reasonably requested by Customer. Company will use reasonable endeavors to assist Customer in investigating the Security Incident and mitigating, where possible, the adverse effects of any Security Incident.

8. Security Assessments and Audits

8.1 Company audits its compliance with data protection and information security standards on a regular basis. Such audits are conducted by Company's internal audit team or by third party auditors engaged by Company, and will result in the generation of an audit report **("Report"),** which will be Company's confidential information.

8.2 Company shall, upon reasonable and written notice and subject to obligations of confidentiality, allow its data processing proceduresand documentation to be inspected, no more than once a year and in normal business hours, by Customer (or its designee), at Customer's expense, in order to ascertain compliance with this DPA and Data Protection Law. Company shall cooperate in good faith with audit requests by providing access to relevant knowledgeable personnel and documentation.

8.3 At Customer's written request, and subject to obligations of confidentiality, Company may satisfy the requirements set out in this section by providing Customer with a copy of the Report so that Customer can reasonably verify Company's compliance with its obligations under this DPA and Data Protection Law. If Customer wishes to change this instruction regarding the audit, then Customer has the right to request a change to this instruction by sending Company written notice. If Company declines to follow any instruction requested by Customer regarding audits or inspections, Customer is entitled to terminate this DPA and the Agreement.

9. Cooperation and Assistance

9.1 If Company receives any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement, including requests from individuals seeking to exercise their rights under GDPR or CCPA, Company will promptly redirect the request to Customer. Company will not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If Company is required to respond to such a request, Company will promptly notify Customer and provide Customer with a copy of the request, unless legally prohibited from doing so. The Customer is responsible for verifying that the requestor is the data subject whose

information is being sought. Company bears no responsibility for information provided in good faith to Customer in reliance on this subsection.

9.2 If Company receives a legally binding request for the disclosure of Personal Data which is subject to this DPA, Company shall (to the extent legally permitted) notify Customer upon receipt of such order, demand, or request. It is hereby clarified however that if no such response is received from Customer within three (3) business days (or otherwise any shorter period as dictated by the relevant law or authority), Company shall be entitled to provide such information.

9.3 Notwithstanding the foregoing, Company will cooperate with Customer with respect to any action taken by it pursuant to such order, demand or request, including ensuring that confidential treatment will be accorded to such disclosed Personal Data. Customer shall cover all costs incurred by Company in connection with its provision of such assistance.

9.4 Upon reasonable notice, Company shall:

(A) Taking into account the nature of the processing, provide reasonable assistance to the Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Customer's obligation to respond to requests for exercising Data Subject's rights, at Customer's expense;

(B) Provide reasonable assistance to the Customer in ensuring Customer's compliance with its obligation to carry out data protection impact assessments or prior consultations with data protection authorities with respect to the processing of Personal Data, provided, however, that if such assistance entails material costs or expenses to Company, the Parties shall first come to agreement on Customer reimbursing Company for such costs and expenses.

9.5 Customer agrees to exercise any right it may have to conduct an audit or inspection, including under the Standard Contractual Clauses if they apply, by instructing Company to carry out the audit described herein.

10. Use of Sub-Processors

10.1 Customer provides a general authorization to Company to appoint (and permit each Sub-Processor appointed in accordance with this Clause to appoint) Processors and/or Sub Processors in accordance with this Clause.

10.2 Company may continue to use those Processors and/or Sub Processors already engaged by Company as at the date of this Agreement, subject to Company, in each case as soon as practicable, meeting the obligations set out in this Clause.

10.3 Company can at anytime appoint a new Processor and/or Sub-Processor provided that Customer is given ten (10) days' prior notice and the Customer does not legitimately object to such changes within that timeframe. Legitimate objections must contain reasonable and documented grounds relating to a Processor and/or Sub-Processor's non-compliance with Data Protection Law.

10.4 With respect to each Processor and/or sub-processor, Company shall ensure that the arrangement between Company and the Processor and/or Sub Processor is governed by a written contract including terms which offer at least the same level of protection as those set out in this Agreement and meet the requirements of article 28 (3) of the GDPR and/or of the CCPA (as applicable);

10.5 Company will be responsible for any acts, errors or omissions by its Sub-Processors, which may cause Company to breach any of its obligations under this DPA and Data Protection Law.

10.6 Company will only disclose Personal Data to Sub-Processors for the specific purposes of carrying out the Services on Company's behalf.

10.7 Company does not sell or disclose Personal Data to third parties for commercial purposes, except as required under applicable laws.

11. Transfer of EEA resident Personal Data outside the EEA

11.1 For EU data transfers directly to countries outside the European Economic Area, that have not been recognized by the EU Commission as a country which ensures an adequate level of protection within the meaning of Applicable Data Protection Law, the Controller and Processor, as applicable, shall be deemed to enter and have implemented the Standard Contractual Clauses, which are incorporated herein by reference, together with Annexes 1-3.

The Parties agree that for the purpose of transfer of Personal Data between Data Importers and Data Exporters, the following shall apply:

11.2 Clause 7 of the Standard Contractual Clauses shall not be applicable.

- In Clause 9, option 2 shall apply. Importer shall inform Exporter in writing of any intended addition or replacement of sub-processors at least seven (7) days in advance.
- In Clause 11, data subjects shall not be able to lodge a complaint with an independent dispute resolution body.
- In Clause 17, option 1 shall apply. The Parties agree that the clauses shall be governed by the law of Ireland; and
- In Clause 18(b) the Parties choose the courts of Dublin, Ireland as their choice of forum and jurisdiction
- Schedules 1-3 of this DPA shall serve as Annex 1-3 respectively.

11.3 For UK data transfers directly to countries outside the UK, that have not been recognized by the EU Commission as a country which ensures an adequate level of protection within the meaning of Applicable Data Protection Law, the Controller and Processor, as applicable, shall be deemed to enter and have implemented the UK Standard Contractual Clauses, which are incorporated herein by reference, and the following shall apply:

- All the information provided under the Standard Contractual Clauses shall apply to the UK Standard Contractual Clauses with the necessary changes per the requirement of the UK Standard Contractual Clauses. Annexes 1A, 1B and 2 to the UK Addendum shall be replaced with Schedules 1-3 below, respectively.

- In Table 4 of the UK Standard Contractual Clauses, either party may terminate the agreement.

.

12. Data Retention and Destruction

12.1 Company will only retain Personal Data for the duration of the Agreement or as required to perform its obligations under the Agreement, or has otherwise required to do so under applicable laws or regulations. Following expiration or termination of the Agreement or upon Customer's request, Company will delete or return to Customer all Personal Data in its possession as provided in the Agreement, except to the extent Company is required under applicable laws to retain the Personal Data. The terms of this DPA will continue to apply to such Personal Data. This section shall not apply to the activities that are the subject matter of section 3.1 herein.

12.2 Upon Customer's request, Company shall provide Customer with a certificate confirming that it has fully complied with clause 12.1.

12.3 Notwithstanding the foregoing, Company shall be entitled to maintain Personal Data following the termination of this Agreement for statistical and/or financial purposes provided always that Company maintains such Personal Data on an aggregated basis or otherwise after having removed all personally identifiable attributes from such Personal data.

12.4 Notwithstanding the foregoing, Company shall be entitled to retain Personal Data solely for the establishment or exercise of legal claims, and/or in aggregated and anonymized form, for whatever purpose.

13. General

13.1 Any claims brought under this DPA will be subject to the terms and conditions of the Agreement, including the exclusions and limitations set forth in the Agreement.

13.2 In the event of a conflict between the Agreement (or any document referred to therein) and this DPA, the provisions of this DPA shall prevail.

13.3 Changes. Either Party may change this DPA if the change is required to comply with Data Protection Law, a court order or guidance issued by a governmental regulator or agency, provided that such change does not: (i) seek to alter the categorization of the Company as the Data Processor; (ii) expand the scope of, or remove any restrictions on, either Party's rights to use or otherwise process Personal Data; or (iii) have a material adverse impact on Customer.

13.4 Notification of Changes. If either Party intends to change this DPA under this section **("Changing Party"),** and such change will have a material adverse impact on the other Party, then the Changing Party will use commercially reasonable efforts to inform the other Party at least 30 days (or such shorter period as may be required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency) before the change will take effect.

By signature, the Parties acknowledge that they have read and understood the terms of this DPA and agree to be legally bound by it:

Customer	**Company**
Signature	Signature _____
Print Name	Print Name _____
Title	Title _____
Date	Date _____

frontegg

Schedule 1

A. Identification of Parties

"Data Exporter": Customer

"Data Importer": Company

B. Description of Transfer

Data Subjects

The Personal Data transferred concern the following categories of Data Subjects (please specify):

☒ end-users

☒ employees

☐ customers

☐ Other: _____

Categories of Personal Data

The Personal Data transferred concern the following categories of data (please specify):

☒ Contact Information

☐ Financial and payment data (e.g. credit card number, bank account, transactions)

☐ Governmental IDs (passport, driver's license)

☒ Device identifiers and internet or electronic network activity (IP addresses, GAID/IDFA, browsing history, timestamps)

☐ Geo-location information

☐ Other: _____

Special Categories of Data (if appropriate)

The Personal Data transferred concern the following special categories of data (please specify):

☒ None

☐ Genetic or biometric data

☐ Health data

☐ Racial or ethnic origin

☐ Political opinions, religious or philosophical beliefs

☐ Other: _____

The frequency of the transfer

The frequency of the transfer:

☐ One-off

☒ Continuous

☐ Other: _____

Nature of the processing

☒Collection

☐ Recording

☐ Organization or structuring

☒ Storage

☐ Adaptation or alteration

☐ Retrieval

☐ Consultation

☐ Disclosure, dissemination or otherwise making available

☒ Analysis

☐ Erasure or destruction

☐ Other: _____

Purpose of the transfer and further processing

As defined in the main agreement between the Parties.

Retention period

Personal Data will be retained for the term of the main agreement, unless Exporter request otherwise.

Supervisory Authority

The Supervisory Authority will be set in accordance with the provisions of Clause 13 of the Standard Contractual Clauses.

Schedule 2

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached

As described in the Company's Trust Center located here - https://frontegg.com/trust-center.

Schedule 3

Pre-approved Sub-processors

As detailed in the Company's website:
https://frontegg.com/trust-center/privacy/sub-processors