hiver

EU GDPR

CUSTOMER DATA PROCESSING ADDENDUM

WHO SHOULD EXECUTE THIS DPA

If you have determined that you qualify as a data controller under the GDPR, and need a data processing addendum (DPA) in place with vendors that process personal data on your behalf, you may execute this DPA.

Our GDPR compliant DPA is attached and ready for your signature in accordance with the instructions below.

HOW TO EXECUTE THIS DPA

1. This DPA consists of two parts: the main body of the DPA and Annexes A, B, C and D.
2. This DPA has been pre-signed on behalf of Hiver.
3. To complete this DPA, Customer must complete the information in the signature box and sign on Page 11
4. Send the completed and signed DPA to Hiver by e-mail, indicating the Customer's Legal Name to dpa@hiverhq.com

Upon receipt of the validly completed DPA by Hiver at this e-mail address, this DPA will become legally binding.

EU GDPR
DATA PROCESSING ADDENDUM
(*Version 1.3*)

Data Processing Addendum ("**DPA**"), forms part of the Subscription Agreement between Grexit, Inc. d/b/a Hiver ("**Hiver**") and the undersigned customer of Hiver ("**Customer**") and shall be effective on the date both parties execute this DPA (**Effective Date**"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

Hiver and Customer are collectively referred to as “**Parties**” and individually as “**Party**”.

1. Definitions

"**Main Agreement**" means Hiver’s Terms of Service (available at https://hiverhq.com/terms) or other written or electronic agreement by and between Hiver and the Customer, which govern the provision of the Services to Customer, as such terms may be updated by Hiver from time to time.

"**Control**" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "**Controlled**" shall be construed accordingly.

"**Customer Data**" means any Personal Data that Hiver processes on behalf of Customer as a Data Processor in the course of providing Services, as more particularly described in this DPA.

"**Data Protection Laws**" means all data protection and privacy laws applicable to the processing of Personal Data under the Main Agreement, including, where applicable, EU Data Protection Law.

"**Data Controller**" means an entity that determines the purposes and means of the processing of Personal Data.

"**Data Processor**" means an entity that processes Personal Data on behalf of a Data Controller.

“**Data Subject**” means the individual to whom Personal Data relates.

"**EU Data Protection Law**" means on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council 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) ("**GDPR**").

"**EEA**" means, for the purposes of this DPA, the European Economic Area, United Kingdom and Switzerland.

"**Personal Data**" means any information relating to an identified or identifiable natural person.

"**Processing**" has the meaning given to it in the GDPR and "**process**", "**processes**" and "**processed**" shall be interpreted accordingly.

"**Security Incident**" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data transmitted, stored or otherwise processed.

"**Services**" means any product or service provided by Hiver (including its Indian subsidiary namely Grexit Software Private Limited) to Customer pursuant to the Main Agreement.

"**Standard Contractual Clauses**" means the agreement executed by and between Customer and Hiver and attached hereto as Annex D pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

"**Sub-processor**" means any third-party Data Processor engaged by Hiver to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA.

2. Relationship with the Agreement

2.1 This DPA is an addendum to and forms part of the Main Agreement. The Customer entity signing this DPA must be the same as the Customer entity party to the Main Agreement.

2.2 The parties agree that DPA shall replace any existing DPA the parties may have previously entered into in connection with the Services.

2.3 If there is a conflict between the Main Agreement and this DPA, only pertaining to the subject matter of this DPA, the terms of this DPA will control.

2.4 Any claims brought under or in connection with this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Main Agreement.

2.5 Any claims against Hiver under this DPA shall be brought solely by the entity that is a party to the Main Agreement. In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise. Customer further agrees that any regulatory penalties incurred by Hiver in relation to the Customer Data that arise as a result of, or in connection with, Customer’s failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce Hiver’s liability under the Main Agreement as if it were liability to the Customer under the Main Agreement.

2.6 No one other than a party to this DPA, its successors and permitted assignees shall have any right to enforce any of its terms.

2.7 This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Main Agreement, unless required otherwise by applicable Data Protection Laws.

3. Scope and Applicability of this DPA

3.1 This DPA applies where and only to the extent that Hiver processes Customer Data that originates from the EEA and/or that is otherwise subject to EU Data Protection Law on behalf of Customer as Data Processor in the course of providing Services pursuant to the Main Agreement.

3.2 Part A (being Section 4 – 8 (inclusive) of this DPA, as well as Annexes A, B and C of this DPA) shall apply to the processing of Customer Data within the scope of this DPA from the Effective Date.

3.3 Part B (being Sections 9-15 (inclusive) of this DPA) shall apply to the processing of Customer Data within the scope of the DPA from and including 25th May 2018. For the avoidance of doubt, Part B shall apply in addition to, and not in substitution for, the terms in Part A.

3.4 With respect to the processing of Personal Data falling within the scope of Part B:

(a) the terms of Part B shall apply in addition to, and not in substitution of, the terms in Part A; and

(b) to the extent there is any conflict between the provisions in Part A and Part B, the provisions in Part B shall take priority from and including 25 May 2018.

3.5 Notwithstanding anything in this DPA, Hiver will have the right to collect, extract, compile, synthesize and analyze non-personally identifiable data or information resulting from Customer’s use or operation of the Services (“**Service Data**”) including, by way of example and without limitation, information relating to Service usage pattern by the Customer. To the extent any Service Data is collected or generated by Hiver, such data will be solely owned by Hiver and may be used by Hiver for any lawful business purpose without a duty of accounting to Customer or its recipients, provided that such data is used only in an aggregated form, without directly identifying any person. For the avoidance of doubt, this DPA will not apply to Service Data.

Part A: General Data Protection Obligations

4. Roles and Scope of Processing

4.1 **Role of the Parties**. As between Hiver and Customer, Customer is the Data Controller of Customer Data, and Hiver shall process Customer Data only as a Data Processor as described in **Annex A** acting on behalf of Customer.

4.2 **Customer Processing of Customer Data**. Customer agrees that (i) it shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with Data Protection Laws and agrees to review and update such measures from time to time; (ii) it shall comply with its obligations as a Data Controller under Data Protection Laws in respect of its processing of Customer Data and any processing instructions it issues to Hiver/its staff/its Sub-processors; (iii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under Data Protection Laws for Hiver to process Customer Data and provide the Services pursuant to the Main Agreement and this DPA; (iv) it shall implement appropriate data protection policies, where it performs any partial processing activities; (v) prepare codes of conduct with regard to fair and transparent processing, collection of personal data, information provided to the public and/or to data subjects, exercise of rights of data subjects, dispute resolution procedures for resolving disputes with data subjects without prejudice to the rights of data subjects under GDPR; (vi) it shall designate, if necessary, in writing a representative in the Union on all issues related to processing, if it is not established in the European Union. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

4.3 **Hiver Processing of Customer Data**. Hiver shall treat Personal Data as confidential information and shall process Customer Data only for the purposes described in **Annex A** and only in accordance with Customer’s documented lawful instructions, including with regard to transfers of personal data to a third country or an international organization (unless required to do so by any local and/or applicable laws). The parties agree that this DPA and the Main Agreement set out the Customer’s complete and final instructions to Hiver in relation to the processing of Customer Data and processing outside the scope of these instructions (if any) shall require prior written agreement between Customer and Hiver.

4.4 Details of Data Processing

A description of the nature and purposes of the processing, the types of Personal Data, categories of data subjects, and the duration of the processing are set out further in **Annex A**.

4.5 Notwithstanding anything to the contrary in the Main Agreement (including this DPA), Customer acknowledges that Hiver shall have a right to use and disclose data (as mentioned in **Annex A**) relating to the operation, support and/or use of the Services for its legitimate business purposes, such as billing, account management, technical support, product development and sales and marketing. To the extent any such data is considered Personal Data under Data Protection Laws, Hiver is the Data Controller of such data and accordingly shall process such data in accordance with the Hiver Privacy Policy (https://hiverhq.com.com/privacy) and Data Protection Laws.

4.6 Compliance

Customer shall be solely responsible for ensuring that:

(i) it has complied, and will continue to comply, with all applicable laws relating to privacy and data protection, including EU Data Protection Legislation, in its use of the Services and its own processing of Personal Data (except as otherwise required by applicable law);

(ii) it has, and will continue to have, the right to transfer, or provide access to, the Personal Data to Hiver for processing in accordance with the terms of the Main Agreement and this DPA;

(iii) it notifies an appropriate supervisory authority about personal data breach, without undue delay, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Such notification shall at least (at once or in phases): (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;(b) communicate the name and contact details of some contact point where more information can be obtained;(c) describe the likely consequences of the personal data breach;(d) describe the measures taken or proposed to be taken by the Customer to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;

(iv) it communicates the data subject (unless not necessary), without undue delay, when a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. Such communication shall describe in clear and plain language the nature of the personal data breach;

(v) it maintains a record of processing activities under its responsibility, containing information as per Data Protection Laws;

5. Subprocessing

5.1 **Authorized Sub-processors**. Customer acknowledges and agrees that Hiver may engage Sub-processors to process Customer Data on Customer's behalf. The Sub-processors currently engaged by Hiver and authorized by Customer are listed in **Annex B**.

5.2 **Sub-processor Obligations**. Hiver shall:

(i) enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Customer Data to the standard required by Data Protection Laws and Customer’s documented lawful instructions;

(ii) restrict the Sub-processor’s access to Personal Data only to what is necessary to perform the subcontracted services; and

(iii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause Hiver to breach any of its obligations under this DPA.

6. Security

6.1 **Security Measures**. Hiver shall implement and maintain appropriate technical and organizational security measures to protect Customer Data from Security Incidents and to preserve the security and confidentiality of the Customer Data, in accordance with Hiver's security standards described in **Annex C** ("**Security Measures**").

6.2 **Updates to Security Measures**. Customer is responsible for reviewing the information made available by Hiver relating to data security and making an independent determination as to whether the Services meet Customer’s requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that Hiver 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 purchased by the Customer.

6.3 **Customer Responsibilities**. Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Customer Data when it transits to and from the Services.

7. Security Reports and Audits

7.1 Customer acknowledges that Hiver uses external auditors to comprehensively assess security of the systems used by Hiver to provide data processing services. At Customer's written request, Hiver will (on a confidential basis) provide Customer with a summary of its audit report(s) ("**Report**") so that the Customer can verify Hiver's compliance. The Customer further acknowledges that these audits (i) are performed at least once each year; and (ii) are conducted by auditors selected by Hiver, but otherwise conducted with all due and necessary independence and professionalism.

7.2 Hiver shall also provide written responses (on a confidential basis) to all reasonable requests for information made by Customer, including responses to information security and audit questionnaires that are necessary to confirm Hiver's compliance with this DPA, provided that Customer shall not exercise this right more than twice per year.

8. International Transfers

8.1 **Data center locations**. Hiver may transfer and process Customer Data at its data center located in the United States or anywhere in the world where its Sub-processors maintain data processing operations. Hiver shall at all times provide an adequate level of protection for the Customer Data processed, in accordance with the requirements of Data Protection Laws.

8.2 **Standard Contractual Clause.** To the extent that Hiver processes any Customer Data protected by EU Data Protection Law under the Main Agreement and/or that originates from the EEA, the UK, or the Switzerland in a country that has not been designated by the European Commission or Swiss Federal Data Protection Authority (as applicable) as providing an adequate level of protection for Personal Data, the parties acknowledge that Hiver shall be deemed to provide adequate protection (within the meaning of EU Data Protection Law) for any such Customer Data by virtue of having self-certified its compliance with the Standard Contractual Clauses.

Part B: GDPR Obligations

9. Additional Security

9.1 **Confidentiality of processing**. Hiver shall ensure that any person who is authorized by Hiver to process Customer Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

9.2 **Security of Processing**. The Customer and Hiver shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including but not limited to: (i) the encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

9.3 **Security Incident Response**. Upon becoming aware of a Security Incident, Hiver shall notify Customer without undue delay (but in any event no later than 72 hours) and shall provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer. Hiver shall make reasonable endeavors to identify the cause of such Security Incident and take those steps as Hiver deems necessary and reasonable in order to remediate the cause of such a Security Incident to the extent the remediation is within Hiver’s reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer’s Users.

10. Changes to Sub-processors

10.1 Hiver shall (i) provide an up-to-date list of the Sub-processors it has appointed upon written request from Customer; and (ii) notify Customer (for which e-mail shall suffice) if it adds or removes Sub-processors at least 10 days prior to any such changes.

10.2 Customer may object in writing to Hiver’s appointment of a new Sub-processor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such an event, the parties shall discuss such concerns in good faith with a view to achieving resolution. If this is not possible, Customer may suspend or terminate the Main Agreement (without prejudice to any fees incurred by Customer prior to suspension or termination).

11. Return or Deletion of Data

11.1 Upon termination or expiration of the Main Agreement, Hiver shall (at Customer's election) delete or return to Customer all Customer Data (including copies) in its possession or control, save that this requirement shall not apply to the extent Hiver is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data Hiver shall securely isolate and protect from any further processing, except to the extent required by applicable law.

12. Cooperation

12.1 The Services provide Customer with a number of controls that Customer may use to retrieve, correct or delete Customer Data, which Customer may use in connection with its obligations under the GDPR, including its obligations relating to responding to requests from data subjects or applicable data protection authorities. To the extent that Customer is unable to independently access the relevant Customer Data within the Services, Hiver shall (at Customer's expense, to the extent legally permitted), taking into account the nature of processing, provide reasonable cooperation to assist Customer by appropriate technical and organizational measures to respond to any requests from individuals, data subjects or applicable data protection authorities relating to the processing of Personal Data under the Main Agreement. In the event that any such request is made directly to Hiver, Hiver shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If Hiver is required to respond to such a request, Hiver shall promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

12.2 If a law enforcement agency sends Hiver a demand for Customer Data (for example, through a subpoena or court order), Hiver shall attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Hiver may provide Customer’s basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then Hiver shall give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Hiver is legally prohibited from doing so.

12.3 To the extent Hiver is required under EU Data Protection Law, Hiver shall (at Customer's expense) assist and provide reasonably requested information regarding the Services to enable the Customer to implement security of processing, to notify/ communicate personal data breach, to conduct audits/inspections, to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

13. Limitation of Liability

13.1 Hiver’s liability under or in connection with this DPA is subject to the limitations on liability and any indemnity clause contained in the Main Agreement.

14. Governing Law

14.1 Without prejudice to Clause 9 (Governing Law) of the Standard Contractual Clauses, the Parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Main Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of Santa Clara County, California.

15. Mediation and Jurisdiction

15.1 Without prejudice to Clause 7 (Mediation and Jurisdiction) of the Standard Contractual Clauses, Hiver agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the clauses, Hiver will accept the decision of the data subject:(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;(b) to refer the dispute to the

IN WITNESS WHEREOF, the parties have caused this DPA to be executed by their authorized representative:

On behalf of Customer:

Customer Legal Name:____________________

Title: ____________________

Date: ____________________

Signature: ____________________

On behalf of Grexit, Inc. d/b/a Hiver

Name: Nitesh Nandy

Title: Co-Founder

Date: 7/13/2022

Signature: ____________________

DocuSigned by:

8ED541C59C74460...

STANDARD CONTRACTUAL CLAUSES FOR THIRD-COUNTRY TRANSFERS
Module 2 (transfer from Controller to Processor)

§ 1. Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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) for the transfer of personal data to a third country.

(b) The Parties:
(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter ‘entity/ies’) transferring the personal data, as listed in Annex I.A (hereinafter each ‘data exporter’), and
(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each ‘data importer’)
have agreed to these standard contractual clauses (hereinafter: ‘Clauses’).

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

§ 2. Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

§ 3. Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii) Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e);
(iii) Clause 9(a), (c), (d) and (e);
(iv) Clause 12(a), (d) and (f);
(v) Clause 13; (vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18(a) and (b);.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

§ 4. Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

§ 5. Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

§ 6. Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

§ 7. Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

§ 8. Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses.

§ 8.1. Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

§ 8.2. Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

§ 8.3. Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

§ 8.4. Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

§ 8.5. Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

§ 8.6. Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context, and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In the case of pseudonymization, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organizational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management, and monitoring of the contract. It shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and an approximate number of data subjects and personal data records concerned), its likely consequences, and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular, to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

§ 8.7. Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offenses (hereinafter ‘sensitive data’), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

§ 8.8. Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter ‘onward transfer’) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise, or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person. Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

§ 8.9. Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

§ 9. Use of sub-processors

(a) The data importer has the data exporter's general authorization for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 10 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfills its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the subprocessor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfill its obligations under that contract.

(e) The data importer shall agree to a third-party beneficiary clause with the sub-processor whereby – in the event, that the data importer has factually disappeared, ceased to exist in law, or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

§ 10. Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorized to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organizational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

§ 11. Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

§ 12. Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processors), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

§ 13. Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as the competent

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as the competent supervisory authority.

[Where the data exporter is not established in an EU Member State but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, as indicated in Annex I.C, shall act as the competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

§ 14. Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679 are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of the processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical, or organizational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfill its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

§ 15. Obligations of the data importer in case of access by public authorities

§ 15.1. Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them at the request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

§ 15.2. Review of legality and data minimization

(a) The data importer agrees to review the legality of the request for disclosure, in particular, whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

§ 16. Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

§ 17. Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Santa Clara County, California.

§ 18. Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Santa Clara County, California.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE: It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

Annex 1

A. LIST OF PARTIES

Data exporter(s):

[*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

1. Name: . . . .

Address: . . . .

Contact person's name, position and contact details: . . . .

Activities relevant to the data transferred under these Clauses: . . . .

Signature and date: . . . .

Role (controller/processor): . . . .

2. Name: . . . .

Address: . . . .

Contact person's name, position and contact details: . . . .

Activities relevant to the data transferred under these Clauses: . . . .

Signature and date: . . . .

Role (controller/processor): . . . .

Data importer(s):

[*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*]

1. Name: **Grexit, Inc.**

Address: **Suite 203, 2880 Zanker Rd, San Jose 95134**

Contact person's name, position, and contact details: **Nitesh Nandy, Co-Founder, nitesh@hiverhq.com**

Activities relevant to the data transferred under these Clauses: . . . .

Signature and date: . . . . DocuSigned by: 8ED541C59C74460... 7/13/2022 . . . .

Role (controller/processor): **Processor**

2. Name: . . . .

Address: . . . .

Contact person's name, position and contact details: . . . .

Activities relevant to the data transferred under these Clauses: . . . .

Signature and date: . . . .

Role (controller/processor): . . . .

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Any individual accessing and/or using the Services through the Customer's account ("Users"); and any individual whose information is stored on or collected via the Services.

Categories of personal data transferred

1. Customer contact information (name, e-mail address, phone number, username); billing information (credit card, account details, billing address); and
2. e-mail information (subject of e-mail, e-mail Message-ID, sender's e-mail address); and
3. Any other personal data that the Customer chooses to store in the e-mail notes, e-mail templates, and shared drafts feature. This personal data transferred to Hiver is determined and controlled by the Customer at its sole discretion. Hiver has no control over the sensitivity of the personal data stored and processed through e-mail notes, e-mail templates, and shared drafts feature.

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 limitations, 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.

. . . .
. . . .

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

As between Hiver and Customer, the duration of the data processing under this DPA is until the termination of the Main Agreement in accordance with its terms.

Nature and Purpose(s) of the data transfer and further processing

Hiver provides an e-mail collaboration platform that helps teams work more efficiently. Hiver runs on top of the Customer's existing e-mail provider to provide additional services which enable collaboration. The purpose of the data processing under this DPA is the provision of the Services to the Customer and the performance of Hiver's obligations under the Main Agreement (including this DPA) or as otherwise agreed by the parties.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

. . . .
. . . .

For transfers to (sub-) processors, also specify the subject matter, nature, and duration of the processing

Hiver uses a range of third-party Sub-processors to assist it in providing the Services (as described in the Main Agreement). Hiver uses these sub-processors to provide cloud hosting and storage services; content delivery and analytics services; assist in providing customer support; as well as incident tracking, response, diagnosis, and resolution services. An updated list of these Sub-processors can be found at https://hiverhq.com/third-party-subprocessors.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13 . . . .
. . . .
. . . .

ANNEX C

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE: The technical and organizational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

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.

A description of the technical and organizational security measures implemented by Hiver is available at this link - https://hiverhq.com/security-center