Data Processing Addendum

This Data Processing Addendum ("**DPA**"), forms part of the Agreement or other written or electronic agreement between Pleo Technologies A/S ("**Pleo**") and Customer for the purchase of Services from Pleo. By signing the Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Affiliates. This DPA shall be effective on the date both parties have executed this DPA ("**Effective Date**"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

How to execute this DPA

This DPA consists of two parts: Part A (General Data Protection Obligations) and Part B (GDPR Obligations from 25 May 2018). To complete this DPA customer must:

1. Fill in correct information in the signature box and sign on Page 9.
2. Send the completed and signed DPA to Pleo by email, including the Customer's legal name to dataprocessingaddendum@pleo.io. The email must be sent by the Customer's Pleo account administrator

Upon receipt of the validly sent and completed DPA by Pleo, this DPA will become legally binding.

How this DPA applies

If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to, and forms part of, the Agreement. In such case, the Pleo entity that is party to the Agreement is party to this DPA.

If the Customer entity signing this DPA is not a party to the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this DPA.

1. Definitions
"**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.

"**Agreement**" means Pleo's Terms of Service/Terms and Conditions, which govern the provision of the Services to Customer, as such terms may be updated by Pleo 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 Pleo 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 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.

"**EU Data Protection Law**" means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data ("Directive") and 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"); and (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector and applicable national implementations of it (as may be amended, superseded or replaced).

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

"**Group**" means any and all Affiliates that are part of an entity's corporate group.

"**Personal Data**" means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data.

"**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.

"**Services**" means any product or service provided by Pleo to Customer pursuant to the Agreement.

"**Subprocessor**" means any Data Processor engaged by Pleo or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA. Subprocessors may include third parties or members of the Pleo Group.

“Supervisory Authority” means an independent public authority which is established by an EU Member State pursuant to the GDPR.

2. Relationship with the Agreement

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

2.2 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

2.3 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 Agreement.

2.4 Any claims against Pleo or its Affiliates under this DPA shall be brought solely against the entity that is a party to the 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 Pleo 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 Pleo’s liability under the Agreement as if it were liability to the Customer under the Agreement.

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

2.6 This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the 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 Pleo 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 Agreement.

3.2 Part A (being Section 4 – 8 (inclusive) 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 912 (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.

Part A: General Data Protection Obligations

4. Roles and Scope of Processing

4.1 Role of the Parties. As between Pleo and Customer, Customer is the Data Controller of Customer Data, and Pleo shall process Customer Data only as a Data Processor acting on behalf of Customer.

4.2 Customer Processing of Customer Data. Customer agrees that (i) 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 Pleo; and (ii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under Data Protection Laws for Pleo to process Customer Data and provide the Services pursuant to the Agreement and this DPA.

4.3 Pleo Processing of Customer Data. Pleo shall process Customer Data mainly for the purposes described in this DPA and only in accordance with Customer's documented lawful instructions. The parties agree that this DPA and the Agreement set out the Customer's complete and final instructions to Pleo 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 Pleo.

4.4 Pleo will immediately inform the Customer if, in Pleo's opinion, any given instruction infringes on or violates the GDPR, or other Union or member state data protection provisions.

4.5 Details of Data Processing:

(a) Subject matter: The subject matter of the data processing under this DPA is the Customer Data.

(b) Duration: As between Pleo and Customer, the duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms.

(c) Purpose: The purpose of the data processing under this DPA is the provision of the Services to the Customer and the performance of Pleo's obligations under the Agreement (including this DPA) or as otherwise agreed by the parties.

(d) Nature of the processing: Pleo provides an expense management service and platform and other related services, as described in the Agreement.

(e) Categories of data subjects: Any individual accessing and/or using the Services through the Customer's account ("Users"); third parties with whom Customer or Customer's Users have a commercial or business relationship ("Third Parties").

(f) Types of Customer Data:
(i) Customer and Users: identification and contact data (name, address, title, contact details, username); financial information (account details, payment information); employment details (employer, job title, geographic location, area of responsibility).
(ii) Third Parties: Contact details included in email communications processed for bookkeeping or accounting purposes; identity information (name, email address, title, contact details) submitted to Pleo by Customer or Customer's Users.

4.6 Notwithstanding anything to the contrary in the Agreement (including this DPA), Customer acknowledges that Pleo shall have a right to use and disclose data relating to the operation, support and/or use of the Services for its legitimate business purposes, such as billing, account management, technical support and product development. To the extent any such data is considered Personal Data under Data Protection Laws, Pleo is the Data Controller of such data and accordingly shall process such data in accordance with the Pleo Privacy Policy and Data Protection Laws.

4.7 Tracking Technologies. Customer acknowledges that in connection with the performance of the Services, Pleo employs the use of cookies, unique identifiers, web beacons and similar tracking technologies ("Tracking Technologies"). Pleo shall maintain appropriate notice, consent, opt in and opt out mechanisms as are required by Data Protection Laws.

5. Subprocessing

5.1 Authorized Subprocessors. Customer agrees that Pleo may engage Subprocessors to process Customer Data on Customer's behalf.

5.2 Appointment of Subprocessors. Customer acknowledges and agrees that (i) Pleo's Affiliates may be retained as Subprocessors; and (ii) Pleo and Pleo's Affiliates respectively may engage third party Subprocessors in connection with the provision of the Services. Pleo or a Pleo Affiliate has entered into a written agreement with each Subprocessor containing data protection obligations not less protective than those in this Agreement and applicable law with respect to

the protection of Customer Data to the extent applicable to the nature of the Services provided by such Subprocessor.

6. Security

6.1 Security Measures. Pleo shall implement and maintain appropriate technical and organisational security measures to protect Customer Data from Security Incidents and to preserve the security and confidentiality of the Customer Data, in accordance with Pleo's security standards The Security Measures applicable to the Services are described here https://pleo.io/en/privacy (as updated from time to time in accordance with Section 6.2 of this DPA).

6.2 Updates to Security Measures. Customer is responsible for reviewing the information made available by Pleo 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 Pleo 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 in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to the Services.

7. Security Reports and Audits

7.1 Customer acknowledges that Pleo is regularly audited against PCI standards by independent third party auditors and internal auditors, respectively.

7.2 Pleo shall provide written responses (on a confidential basis) to reasonable requests for information made by Customer, including responses to information security and audit questionnaires that are necessary to confirm Pleo's compliance with this DPA, provided that Customer shall not exercise this right more than once per year. Depending on the volume of request, certain lead time is to be expected.

7.3 Upon Customer's request, and subject to the confidentiality obligations set forth in the data processing addendum, Pleo shall make available to Customer that is not a competitor of Pleo (or Customer's independent, third party auditor that is not a competitor of Pleo) information regarding Pleo's compliance with the obligations set forth in the DPA. Customer is entitled to contact Pleo to request an onsite audit of the architecture, systems and procedures relevant to the protection of Personal Data at locations where Personal Data is stored. Customer shall

reimburse Pleo for any time expended by Pleo or its third party Subprocessors for any such onsite audit at Pleo's then current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such onsite audit, Customer and Pleo shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All costs will be documented, and reimbursement rates shall be reasonable, taking into account the resources expended by Pleo, or its third party Subprocessors. Customer shall promptly notify Pleo with information regarding any noncompliance discovered during the course of an audit. This procedure may be instigated a maximum of once per year and with a minimum of ninety (90) days notice to Pleo.

8. International Transfers

8.1 Data center locations. Pleo may transfer and process Customer Data anywhere in the world where Pleo, its Affiliates or its Subprocessors maintain data processing operations. Pleo shall at all times provide an adequate level of protection for the Customer Data processed, in accordance with the requirements of Data Protection Laws. Specifically, Pleo shall ensure a valid legal basis for any such transfer, as outlined in Chapter 5 GDPR and Articles 45-49 thereof.

Part B: GDPR Obligations from 25 May 2018.

9. Additional Security

9.1 Confidentiality of processing. Pleo shall ensure that any person who is authorized by Pleo 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 Incident Response. Upon becoming aware of a Security Incident, Pleo shall notify Customer directly without undue delay and shall provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer.

10. Changes to Subprocessors

10.1 Appointment of Subprocessors.
Customer expressly authorizes Pleo to engage third party subprocessors, in connection with the provision of Services, provided that each subprocessors shall be bound by substantively similar data protection obligations as set out in this DPA. Any such subprocessor will be permitted to obtain Personal Data only to deliver the services Customer has retained Pleo to provide, and they are prohibited from using Personal Data for any other purpose.

10.2 List of Current Subprocessors and Notification of New Subprocessors.

For the purpose of the authorization Section 10.1 Pleo shall make available to Customer the current list of Subprocessors for the Services. This list is available as Annex I to this Addendum and includes the identities of those Sub Processors and their country of location. Upon Customer request, Pleo shall provide notification of a new Subprocessor(s) before authorizing any new Subprocessor(s) to process personal data in connection with the provision of the applicable Services. Customer requests must be sent to dpo@pleo.io.

10.2 Objection Right for New Subprocessors.
Customer may object to Pleo's use of a new Subprocessor by notifying Pleo promptly in writing within five (5) business days after receipt of Pleo's notice in accordance with the mechanism set out in Section 10.1. In the event that Customer objects to a new Subprocessor, as permitted in the preceding sentence, Pleo will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid processing of personal data by the objected to new Subprocessor without unreasonably burdening the Customer. If Pleo is unable to make available such change within a reasonable period of time, which shall not exceed ninety (90) days, Customer may terminate the applicable Agreements with respect only to those Services which cannot be provided by Pleo without the use of the objected to new Subprocessor by providing written notice to Pleo.

11. Return or Deletion of Data

11.1 Upon termination or expiration of the Agreement, Pleo 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 Pleo is required by applicable law to retain some or all of the Customer Data, or to store Customer Data it has archived on backup systems, which Pleo shall securely isolate and protect from any further processing, except to the extent required by applicable law.

12. Rights of data subjects

12.1 Data Subject Requests. Pleo shall, to the extent legally permitted, promptly notify Customer if Pleo receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("Data Subject Request"). Taking into account the nature of the Processing, Pleo shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Pleo shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Pleo is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the

extent legally permitted, Customer shall be responsible for any costs arising from Pleo's provision of such assistance.

13. Cooperation

13.1 The nature of the Services provide Customer with opportunity to retrieve Customer Data, which Customer may use to assist it in connection with its obligations under the GDPR, including its obligations relating to responding to requests from data subjects (as set out in Section 12.1) or applicable data protection authorities.

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

13.3 To the extent Pleo is required under EU Data Protection Law, Pleo shall (at Customer's expense) provide reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

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

Pleo Technologies A/S ("Pleo")

Signature: Federica Erilmi

Print Name: Federica Erilmi

Title: Legal Counsel, DPO

Date: 25.01.2021

Customer:

Signature:_____

Print Name:_____

Title:_____

Date:_____

ANNEX 1

List of sub-processors

Amazon Web Services (EU based data centre in Ireland) - For hosting services
Hupspot. (US Based) - CRM (Customer Relationship Management) system.
Intercom. (US Based) - Customer Support system.
G-Suite (Google - US Based) - cloud computing / email domain provider.
Segment (US Based) - Analytics functionalities.

ANNEX 2

The technical and security measures undertaken by Pleo Technologies A/S include, but are not limited to:

- 2 factors identification
- Secure password generator
- Clear access management and responsibilities with restrict access
- Encryption
- Robust program controls informed by the requirements of the GDPR
- Appropriate reporting structures
- Assessment and evaluation procedures