Data Processing Agreement

Last update: 14 October 2025
Effective as of: 14 October 2025

1. How to execute this DPA 4
2. How this DPA applies 4
3. Relationship with the Master Service Agreement 4
4. Relationship of the parties 5
5. Roles 5
6. Scope of processing 5
7. Sub-processing 6
8. Security 6
9. Security reports and audits 7
10. International transfers 7
11. Return or deletion of data 8
12. Rights of data subjects 8
13. Cooperation 8

SCHEDULE 1 10
SCHEDULE 2 11
SCHEDULE 3 12
ANNEX 1 12
UK standard contractual clauses 15
ANNEX 2 17
Standard contractual clauses 37
SCHEDULE 4 40

Definitions

All capitalized terms not defined in this DPA shall have the meanings set forth in the Master Service Agreement.

Adequate Country	Means a country or territory that is recognized under European Data Protection Laws as providing adequate protection for Personal Data.
Affiliate	Means an entity that directly or indirectly Controls, is Controlled by, or is under common Control with an entity.
Master Service Agreement	Means Pleo's Master Service Agreement, which governs the provision of the Services to Customer, as such terms may be updated by Pleo from time to time.
Applicable Data Protection Laws	Means any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction which relates to the protection of individuals with regard to the Processing of Personal Data to which a party is subject, including but not limited to; the GDPR, UK GDPR and the UK Data Protection Act 2018 and (b) any code of practice or guidance published by the ICO or other applicable Regulator or the European Data Protection Board.
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 Processor in the course of providing Services, as more particularly described in this DPA.
Controller	Means an entity that determines the purposes and Means of the processing of Personal Data.
Processor	Means an entity that processes Personal Data on behalf of a Controller.
Data Subject	Means the identified or identifiable natural person who is the subject of Personal Data.
Data Protection Laws	Means all laws and regulations of the European Union, the European Economic Area, their member states, and the United Kingdom applicable to the processing of Personal Data under the Main Agreement (including, where applicable, (i) 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) (the "EU GDPR"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (the "UK GDPR"); (iii) the e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii), (iii), (iv).
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.
Pleo	Means Pleo Technologies A/S, Pleo Financial Services A/S and Pleo Financial Services UK Ltd jointly.
Processing	Has the meaning given to it in the GDPR and "process", "processes" and "processed" shall be interpreted accordingly. It includes but is not limited to any operation or set of operations which is performed upon Person Data such as transmission, storage, usage, and erasure.
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 Master Service Agreement.

Standard Contractual Clauses	Means contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.
Sub-processor	Means any 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. Sub-processors may include third parties or members of the Pleo Group.
Supervisory Authority	Means any independent public authority responsible for monitoring the application of the Data Protection Laws, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing and to facilitate the free flow of personal data within the United Kingdom and the EU or else (as applicable).
UK Addendum	Means the International Data Transfer Addendum (Version B1.0) issued by the Information Commissioner's Office under s.119 (A) of the UK Data Protection Act 2018, as updated or amended from time to time.

This Data Processing Agreement ("DPA"), forms an integral part of the Master Service Agreement between Pleo and the Customer for the purchase of services from Pleo (in each case as defined below). By executing the DPA, the 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 execute the MSA.

1. How to execute this DPA

The DPA shall be deemed executed at the same time as the execution of the MSA.

2. How this DPA applies

This DPA applies to Pleo's processing of Personal Data under the agreement executed between Pleo Customer for Pleo's provision of the services rendered under or pursuant to the Pleo Master Service Agreement. This DPA is an addendum to and forms an integral part of the Master Service Agreement.

3. Relationship with the Master Service Agreement

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

3.2. Any claims brought under or in connection with this DPA shall be subject to the Master Service Agreement, including but not limited to, the exclusions and limitations set forth in the DPA.

3.3. 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.

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

3.5. 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.

3.6. This DPA will automatically terminate upon expiration or termination of the Master Service Agreement. The parties agree that certain obligations might extend beyond the termination of this DPA in order to comply with legal requirements, such as Anti-Money Laundering requirements.

4. Relationship of the parties

4.1. Pleo as a Processor. The Parties acknowledge and agree that with regards to the processing of Customer Data, Customer may act as a controller or processor and Pleo is a processor. Pleo will process Customer Data in accordance with Customer's instructions as outlined in Section 6 of this DPA.

5. Roles

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

6. Scope of processing

6.1. Customer processing of Customer Data. Customer agrees that (i) it shall comply with its obligations as a 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 solely to the extent required for Pleo to process Customer Data on behalf of Customer as its Processor. Pleo shall be solely responsible for complying with its own obligations under Data Protection Laws in respect of any processing Pleo carries out as a Controller.

6.2. Customer Instructions. Pleo shall process Customer Data for the purposes described in this DPA and only in accordance with Customer's documented lawful instructions. By entering into the Agreement, Customer instructs Pleo to process Customer Data to provide the Services as Processor and pursuant to any other written instructions given by Customer and acknowledged in writing by Pleo as constituting instructions for purposes of this Agreement. Customer acknowledges and agrees that such instruction authorises Pleo to process Customer Data (a) to perform its obligations and exercise its rights under the Agreement; (b) to perform its legal obligations and to establish, exercise or defend legal claims in respect of the Agreement; and (c) to provide the service as described in the Master Service Agreement, including but not limited to billing, account management, technical support. Any processing in which Pleo determines the purposes and means as a controller is outside the scope of Customer's instructions and remains Pleo's sole responsibility.

6.3. Pleo processing of Customer Data. Pleo shall process Customer Data 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 Master Service 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.

6.4. Pleo shall 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.

7. Sub-processing

7.1. Authorized sub-processors. Customer agrees that Pleo may engage sub-processors to process Customer Data on Customer's behalf. Customer expressly authorizes Pleo to engage sub-processors, including Pleo Affiliates acting as sub-processors, in connection with the provision of Services, provided that each sub-processors shall be bound by substantially similar data protection obligations as set out in this DPA. The same obligations shall apply where a Pleo Affiliate acts as a sub-processor. Pleo shall remain liable for any sub-processor it may engage. Pleo confirms that any such sub-processor shall process personal data only in accordance with Pleo's instructions and only for the purposes of delivering the Services Customer has retained and shall be prohibited from processing personal data for any other purpose.

7.2. Appointment of sub-processors. Customer acknowledges and agrees that (i) Pleo's Affiliates may be retained as sub-processors, and (ii) Pleo and Pleo's Affiliates respectively may engage sub-processors in connection with the provision of the Services. Pleo or a Pleo Affiliate has entered into a written agreement with each sub-processor 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 sub-processor. Sub-processors involved in the processing of personal data are subject to Standard Contractual Clauses, as described in Schedule 3. Sub-processors are reviewed and

assessed in accordance with Pleo internal impact assessment. For further information on the sub-processors please refer to Schedule 2, Security Exhibit.

7.3. A list of Pleo's sub-processors. For the purpose of the authorisation Section 7.1 Pleo shall make available to Customer the current list of sub-processors for the Services. Customer consents to Pleo engaging sub-processors to process Customer Data within the Services for the permitted purposes provided that Pleo maintains an up-to-date list of its sub-processors. This list with the sub-processors including their functions and location of the processing of the personal is available at https://www.pleo.io/en/sub-processors and may be updated by Pleo from time to time in accordance with the terms set in this Agreement. Pleo shall provide notification of a new sub-processor(s) before authorising any new sub-processors to process personal data in connection with the provision of the applicable Services at least thirty (30) calendar days before the new sub-processor processes any Customer Data in the email provided in the Order Form.

7.4. Objection Right for new sub-processors. The Customer may object to Pleo's use of a new sub-processor by notifying Pleo promptly without undue delay within 15 days from notice, in writing to dpo@pleo.io. In the event that the Customer objects to a new sub-processor, Pleo will use reasonable efforts to make available to the 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 sub-processor without unreasonably burdening the Customer. If Pleo is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Customer may terminate the Master Service Agreement with respect only to those Services which cannot be provided by Pleo without the use of the objected to new sub-processor by providing written notice to Pleo. If Customer does not provide a timely objection to any new or replacement sub-processor in accordance with this clause 7.4, Customer will be deemed to have consented to the sub-processor and waived its right to object.

8. Security

8.1. Security Measures. Pleo shall maintain appropriate technical and organisational measures for the protection of the security, confidentiality, authenticity and integrity of Customer Data, as described in Schedule 2 of this DPA. Security Measures shall include appropriate administrative, technical, and physical controls, as defined by industry standards. Customer is responsible for determining whether Pleo's Security Measures meet Customer's requirements and legal obligations as prescribed in Art. 28 para (1) of the GDPR.

8.2. Updates to Security Measures. Customer acknowledges that the Security Measures are subject to technical progress and development and that Pleo will improve its security measures and procedures from time to time to reflect process improvements and changing industry practices, provided that no such change will reduce the overall security of the Services.

8.3. Customer Responsibilities. Customer agrees that, except as provided by this DPA, it is responsible for its secure use of the Services, including securing credentials and encrypting Customer Data in transit to the Services. Customer is additionally responsible for securing and backing up copies of Customer Data that are exported and stored outside the Services.

8.4. Security Incident. Pleo maintains security incident management policies and procedures and shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data unless prohibited by applicable law. A delay in giving such notice requested by law enforcement and/or in light of Pleo's legitimate needs to investigate or remediate the matter before providing notice will not constitute an undue delay. Such notices will describe, to the extent possible, details of the Security Incident, including steps taken to mitigate the potential risks and steps Pleo recommends Customer take to address the Security Incident.

Without prejudice to Pleo's obligations, Customer is solely responsible for complying with Security Incident notification laws applicable to Customer and fulfilling any third party notification obligations related to any Security Incidents. Pleo's notification of or response to a Security Incident under this Section will not be construed as an acknowledgement by Pleo of any fault or liability with respect to the Security Incident.

8.5. Pleo shall assist the Customer in ensuring compliance with the GDPR obligations in relation to a personal data breach, taking into account the nature of processing and the information available to Pleo.

8.6. 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), adhere to all safeguards prescribed by law and have received appropriate training on their responsibilities.

9. Security reports and audits

9.1. Pleo shall maintain an audit program to help ensure compliance with the obligations set out in this DPA, including those obligations required by Applicable Data Protection Laws and Regulations. Customer acknowledges that Pleo is regularly audited against PCI standards by independent third party auditors and internal auditors, respectively.

9.2. Customer reserves the right to conduct a full security assessment of Pleo's processing activities including, but not limited to, reviewing security controls, penetration tests, vulnerability tests, and requesting and reviewing documentation (including Reports) related to Pleo's relevant networks, systems, and processes, to identify the strengths and weaknesses of Pleo's existing security controls and to ensure Pleo's compliance with this DPA and the Agreement. An Audit may be conducted by Customer either itself or through a Third-Party Auditor selected by Customer when:
(i) the information available pursuant to section 9.1 is not sufficient to demonstrate compliance with the obligations set out in this DPA and its Schedules;
(ii) Customer has received a notice from Pleo of a Security Incident; or
(iii) such an Audit is required by Applicable Data Protection Laws and regulations or by Customer's competent supervisory authority.

9.3. An Audit shall be conducted by Customer or its Third-Party Auditor:
(i) acting reasonably, in good faith, and in a proportional manner, taking into account the nature and complexity of the services used by Customer;
(ii) up to one time per year with at least three weeks' advance written notice and
(iii) during Pleo's normal business hours, under reasonable duration and shall not unreasonably interfere with Pleo's day-to-day operations. If Pleo's personnel are required to participate in the Audit, Customer shall reimburse Partner's expenses, as mutually agreed upon prior to the commencement of the Audit.

10. International transfers

10.1. Data center locations. Pleo may transfer and process Customer Data where Pleo, its Affiliates or its sub-processors maintain data processing operations, in accordance with section 7. Pleo shall proceed to such transfers only when it is deemed absolutely necessary to provide the Services as described in the Master Service Agreement and only the personal data that is absolutely necessary. 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. Any transfer of personal data to third countries shall only occur on the basis of documented instructions from the Controller and shall always take place in compliance with Chapter V GDPR, the UK Data Protection Act 2018 and internal relevant policies. Particularly, Pleo confirms that any transfer shall only take place when the following safeguards are in place:
(i) adequacy decision adopted by the European Commission pursuant to Article 45(3)
In the absence of a decision pursuant to Article 45(3), or in the case that an adequacy decision is revoked, Pleo shall transfer Customer Data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Such safeguards shall be outlined in the form of Standard Contractual Clauses (SCCs).

In addition to the SCCs or other appropriate transfer mechanism, Pleo shall perform Transfer Impact Assessments (TIAs) as required under Applicable Data Protection Laws and regulations, including the GDPR. For the purposes of transfer of data from the EU to the UK Schedule 3, Annex I shall apply when applicable. For the purposes of transfer of data from the EU to the US or a third country, Schedule 3, Annex II shall apply. These Annexes shall only apply when conditions are met.

If and as long as the country where Customer Data is transferred is subject to an adequacy decision according to Article 45 (3) GDPR, no Standard Contractual Clauses are required. If and when the adequacy decision is repealed or suspended, Schedule 3 shall automatically apply accordingly.

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 back up systems, which Pleo shall securely isolate and protect from any further processing, except to the extent required by applicable law.

11.2. The Customer shall export any transactional data directly through the Pleo application.

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 organisational 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.

12.2. Notwithstanding the foregoing, Customer understands that Pleo may retain Customer Data if required by law, and such data will remain subject to the requirements of this DPA.

13. Cooperation

13.1. The nature of the Services provide Customer with the 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 Customers’ 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.

SCHEDULE 1
Subject matter & details of processing

1. Nature and Purpose of the Processing.

Pleo will process Personal Data as necessary to provide the Services under the Agreement. Pleo does not sell Customer Data (or end user information within such Customer Data) and does not share such end users' information with third parties for compensation or for those third parties' own business interests.

a. Pleo provides an expense management service and platform and other related services, as described in the Agreement. Pleo will process Customer Data as a processor in accordance with Customer's instructions as outlined in Section 6 (Customer Instructions) of this Agreement.

b. 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.

2. Subject Matter of the Processing.

The subject matter of the data processing under this DPA is the Customer Data.

3. Duration of the Processing.

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.

4. 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").

Types of Customer Data:

a. 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);

b. 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.

SCHEDULE 2
Security exhibit

1. Security program.

Pleo will implement and maintain a formal information security program composed of policies, procedures, and controls that govern the processing, storage, transmission and security of Customer Data (the "Security Program"). The Security Program will include industry-standard practices designed to protect Customer Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access.

The Security Program's framework will include physical, technical and organisational measures reasonably designed to protect the Services and the confidentiality, integrity and availability of Customer Data. Pleo may make changes to the Security Program, provided that no such update will reduce the overall level of commitments or protections provided to Customer as described herein.

1.1. Security organization.

Pleo will appoint a Chief Technology Officer, or equivalent executive, to be responsible for coordinating, managing, and monitoring the information security function, policies, and procedures. Pleo will also appoint a Data Protection Officer, or equivalent executive, to be responsible for coordinating, managing, and monitoring the data privacy function, policies, and procedures.

1.2. Policies.

Pleo will implement and maintain information security policies that govern the Security Program. The information security policies will be: (i) documented; (ii) reviewed and approved by management, including after material changes; and (iii) communicated to relevant personnel.

1.3. Risk management.

Pleo will perform information security risk assessments as part of a risk governance program that is established with the objective to regularly test, assess and evaluate the effectiveness of the Security Program. Such assessments will be designed to recognize and assess the impact of risks and implement identified risk remediation or mitigation strategies to address new and evolving security technologies, changes to industry standard practices, and changing security threats.

1.4. Certifications and attestations.

Pleo will establish and maintain sufficient controls to meet certification and attestation for the objectives stated in PCI-DSS and Google CASA (or equivalent standards) for the Security Program. At least once per calendar year, an assessment against such standards and audit methodologies by an independent third-party auditor will be obtained for environments where Customer Data is stored.

2. Security Measures

Physical Security Measures.

2.1. Data centers.

Pleo will ensure that data centers hosting Customer Data will include: (1) physical access restrictions and monitoring that will include a combination of any of the following: multi-zone security, man-traps, appropriate perimeter deterrents (e.g. fencing, berms, guarded gates), on-site guards, biometric controls,

CCTV, and secure cages; and (2) fire detection and fire suppression systems both localized and throughout the data center floor.

2.2. Media.

For deletion of data, Pleo will ensure that an industry standard such as NIST 800-88 (or substantially equivalent) will be used for the deletion of sensitive materials, including Customer Data, before final disposition of such media.

Technical Security Measures.

2.3. Access administration.

Pleo will ensure that access by personnel to Customer Data will be conducted in a manner that: (i) is protected by authentication and authorization mechanisms; (ii) requires personnel to be assigned a unique user account; (iii) restricts the sharing of individual user accounts; (iv) requires strong authentication with complex passwords; (v) ensures accounts are lock-out enabled; (vi) enforces security controls that adhere to the zero trust principle; (vii) requires access privileges be based on job requirements limited to that necessary for the applicable personnel to undertake their duties; (viii) ensures access is revoked upon termination of employment or consulting relationships; and (ix) requires access entitlements be reviewed by management quarterly.

2.4. Logging and monitoring.

Activity and audit logs will be centrally collected, secured in an effort to prevent tampering, and monitored for anomalies by a trained security team.

2.5. Vulnerability management.

Pleo will perform vulnerability scans within the production environment to determine potential vulnerabilities in accordance with then-current security operating procedures, which will be at least quarterly. When software vulnerabilities are revealed and addressed by a vendor patch, the patch will be obtained from the applicable vendor and applied within an appropriate risk-based timeframe in accordance with the standard operating procedure and only after such patch is tested and determined to be safe for installation in production systems.

2.6. Change control.

Changes to the production environment will be reviewed to minimize risk. Such changes will be implemented in accordance with then-current standard operating procedure.

2.7. Configuration management.

Standard hardened configurations for the system components within the production environment will be maintained using industry standard hardening guides.

2.8. Data encryption.

Industry standard encryption will be used to encrypt Customer Data in transit over public networks and at rest in the production environment.

2.9. Secure software development.

Pleo will follow secure software development and code review practices to prevent harm from malware. Software will be developed using secure application development policies and procedures aligned with industry standard practices. Relevant personnel will receive appropriate training regarding secure application development practices.

2.10. Secure code review.

Pleo mandates managerial code review prior to deployment, in accordance with legal obligations. Pleo adheres to the four eyes principle to ensure optimal system integrity, security of sensitive customer information, and minimization of errors or vulnerabilities. Static testing and analysis of code will be performed prior to the deployment of such code to production environments. Vulnerabilities will be addressed in accordance with the then-current software vulnerability management program.

2.11. Data retention.

Pleo will perform regular backups of Customer Data, which will remain highly available and secured against major disruptions. Customer Data will be retained for the duration of the Agreement and, following termination, for a period prescribed by Applicable Laws.

Organisational security measures.

2.12. Personnel security.

Background screening will be performed on all personnel, in accordance with applicable standard operating procedure and subject to Applicable Law.

2.13. Security awareness and training.

Security and privacy awareness training will be provided to all personnel. Such training will be conducted at time of hire and at least annually throughout employment. Additional role-based training will be provided to personnel with access to Customer Data.

2.14. Sub-processor risk management.

Any sub-processor that accesses, stores, processes or transmits Customer Data will be assessed to ensure it has appropriate security and privacy controls. When Pleo engages a sub-processor under this DPA, Pleo and the sub-processor enter into an agreement with data protection terms substantially similar to those contained herein. Each sub-processor agreement must ensure that Pleo is able to meet its obligations to the Customer. In addition to implementing technical and organisational measures to protect personal data, sub-processors must a) notify Pleo in the event of a Security Incident so Pleo may notify the Customer; b) delete data when instructed by Pleo in accordance with the Customer's instructions to Pleo; c) not engage additional sub-processors without authorization; d) not change the location where data is processed; or e) process data in a manner which conflicts with the Customer's instructions to Pleo.

2.15. Data subjects rights.

Pleo will provide assistance to the Customer as may reasonably be required under Applicable Data Protection Laws to respond to requests from individuals to exercise their rights under Applicable Data Protection Laws (e.g., rights of data access, rectification, erasure, restriction, portability and objection).

SCHEDULE 3

The following Annexes will constitute an integral part of the Master Service Agreement and Data Processing Agreement, when and only if applicable.

Any optional clauses contained in the Standard Contractual Clauses are deemed not included shall not be applicable.

ANNEX 1
UK standard contractual clauses

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Table 1: Parties

Exporter (who sends the Restricted Transfer)	Customer as stated in the Master Service Agreement
Importer (who receives the Restricted Transfer)	PLEO TECHNOLOGIES A/S, a company organised and existing under the laws of Denmark having its registered office at Ravnsborg Tværgade 5C 2200 Copenhagen N, registered under enterprise number CVR no. 36 53 86 86, e-mail dpo@pleo.io
Importer Data Subject Contact	Name: Job title: DPO Contact details including email: dpo@pleo.io

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Same as the date of execution of the DPA Reference (if any): This addendum is attached to and forms part of the Data Processing Agreement (DPA) or any other agreement between Customer and Pleo governing the processing of Customer Data (the "DPA"). Unless otherwise defined in 14 this attachment, capitalised terms used in this attachment have the meanings given to them in the DPA. Other identifier (if any): N/A

Table 3: Appendix Information

Appendix Information means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: Located in Annex I of the EU SCC.

Annex 1B: Description of Transfer: Located in Annex II of the EU SCC.

Annex 2: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Located in Annex II of the EU SCC.

Annex 3: List of sub-processors (Modules 2 and 3 only): Located in Schedule 3 of the Data Processing Agreement.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	which Parties may end this Addendum as set out in Section 19: → Importer → Exporter

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum to EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfills the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words: “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”;

c. Clause 6 (Description of the transfer(s)) is replaced with: “The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex 1B where UK Data Protection Laws apply to the data exporter’s processing when making that transfer.”;

d. Clause 8.7(i) of Module 1 is replaced with: “it is to a country benefiting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;

e. Clause 8.8(i) of Modules 2 and 3 is replaced with: “the onward transfer is to a country benefiting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”

f. References to “Regulation (EU) 2016/679”, “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)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;

i. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;

j. Clause 13(a) and Part C of Annex 1 are not used;

k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;

l. In Clause 16(e), subsection (i) is replaced with: “the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;

m. Clause 17 is replaced with: “These Clauses are governed by the laws of England and Wales.”;

n. Clause 18 is replaced with: “Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a. its direct costs of performing its obligations under the Addendum; and/or

b. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its term.

ANNEX 2
Standard contractual clauses

Section 1

Clause 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)1 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 1.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 1.B.

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

Clause 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.

Clause 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. Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

iii. Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Clause 12 - Module One: Clause 12(a) and (d); Modules Two: Clause 12(a), (d) and (f);

iv. (v) Clause 13;

v. Clause 15.1(c), (d) and (e);

vi. Clause 16(e);

vii. Clause 18 - Modules One, Two : Clause 18(a) and (b); Module Four: Clause 18.

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

Clause 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.

Clause 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.

Clause 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 1.B.

Section 2
Obligations of the parties

Clause 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 organisational measures, to satisfy its obligations under these Clauses

MODULE ONE: TRANSFER CONTROLLER TO CONTROLLER

8.1. Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex 1.B. It may only process the personal data for another purpose:

A. where it has obtained the data subject's prior consent;

B. where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

C. where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2. Transparency

A. In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

   i. of its identity and contact details;

   ii. of the categories of personal data processed;

   iii. of the right to obtain a copy of these Clauses;

   iv. where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

B. Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

C. On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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.

D. Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3. Accuracy and data minimisation

A. Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

B. If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

C. The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4. Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

8.5. Security of processing

A. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they 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 subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

B. The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

C. The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

D. 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 personal data breach, including measures to mitigate its possible adverse effects.

E. In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

F. In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

G. The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6. 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 or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7. Onward transfers

The data importer shall not disclose the personal data 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") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

i. it is to a country benefiting 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 of Regulation (EU) 2016/679 with respect to the processing in question;

iii. the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

iv. it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

v. it is necessary in order to protect the vital interests of the data subject or of another natural person; or

vi. where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8. Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9. Documentation and compliance

A. Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.
B. The data importer shall make such documentation available to the competent supervisory authority on request.

MODULE TWO: TRANSFER CONTROLLER TO PROCESSOR

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 organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised 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 pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, 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 organisational 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 authorised 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 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 offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex 1.B.

8.8. Onward transfer

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 defence 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.

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.

8.1. Instructions

A. The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

B. The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

C. The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

D. After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2. Security of processing

A. The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data2, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

B. The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

C. The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3. Documentation and compliance

A. The Parties shall be able to demonstrate compliance with these Clauses.

B. The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9 — Use of sub-processors

A. Option 2: General Written Authorisation
The data importer has the data exporter's general authorisation 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 ten (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.3 The Parties agree that, by complying with this Clause, the data importer fulfils 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 sub-processor'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 a third-party beneficiary clause with the sub-processor whereby - in the event 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.

Clause 10 — Data subject rights

MODULE ONE: TRANSFER CONTROLLER TO CONTROLLER

A. The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

B.

C. In particular, upon request by the data subject the data importer shall, free of charge:

D.

E. provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

F. rectify inaccurate or incomplete data concerning the data subject;

G. erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

H. Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

I. The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter "automated decision"), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

J. inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

K. implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

L. Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

M. The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

N. If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

MODULE TWO: TRANSFER CONTROLLER TO PROCESSOR

O. 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 authorised to do so by the data exporter.

P. 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 organisational 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.

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

MODULE FOUR: TRANSFER PROCESSOR TO CONTROLLER

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 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 authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE ONE: TRANSFER CONTROLLER TO CONTROLLER
MODULE TWO: TRANSFER CONTROLLER TO PROCESSOR

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:

   1. 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;

   2. refer the dispute to the competent courts within the meaning of Clause 18.

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

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

E. 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.

Clause 12 — Liability

MODULE ONE: TRANSFER CONTROLLER TO CONTROLLER
MODULE FOUR: TRANSFER PROCESSOR TO CONTROLLER

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. Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.

C. 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.

D. The Parties agree that if one Party is held liable under paragraph (c), 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.

E. The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

MODULE TWO: TRANSFER CONTROLLER TO PROCESSOR

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-processor), 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.

Clause 13 — Supervision

MODULE ONE: TRANSFER CONTROLLER TO CONTROLLER
MODULE TWO: TRANSFER CONTROLLER TO PROCESSOR

R. [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 competent supervisory authority.

S. 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.

Section 3
Local laws and obligations in case of access by public authorities

Clause 14 — Local laws and practices affecting compliance with the Clauses

MODULE ONE: TRANSFER CONTROLLER TO CONTROLLER

MODULE TWO: TRANSFER CONTROLLER TO PROCESSOR

MODULE FOUR: TRANSFER PROCESSOR TO CONTROLLER (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

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 authorising 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:

    1. 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 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;

    2. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards4;

    3. any relevant contractual, technical or organisational 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 fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational 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.

Clause 15 — Obligations of the data importer in case of access by public authorities

MODULE ONE: TRANSFER CONTROLLER TO CONTROLLER

MODULE TWO: TRANSFER CONTROLLER TO PROCESSOR

MODULE FOUR: TRANSFER PROCESSOR TO CONTROLLER (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

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:

1. 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

2. 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 on 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 © 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 minimisation

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.

Section 4
Final provisions

Clause 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:

   1. 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;

   2. the data importer is in substantial or persistent breach of these Clauses; or

   3. 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. [For Modules One, Two:] 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.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] 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.

Clause 17

MODULE ONE: TRANSFER CONTROLLER TO CONTROLLER

MODULE TWO: TRANSFER CONTROLLER TO PROCESSOR

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 Denmark

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Denmark

Clause 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 the Kingdoms of Denmark.

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.

MODULE FOUR: TRANSFER PROCESSOR TO CONTROLLER

Any dispute arising from these Clauses shall be resolved by the courts of the Republic of Ireland.

Annex 1

A. DESCRIPTION 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]

Name: Customer [INSERT DATA]

Address:

Contact person's name, position and contact details: As stated in the Master Service Agreement Activities relevant to the data transferred under these Clauses: Use of Service pursuant to the Master Service Agreement

Signature and date: This Annex II shall be deemed executed upon execution of the DPA.

Role (controller/processor): Controller

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

Name: Pleo Technologies A/S

Address: Ravnsborg Tværgade 5C 2200 Copenhagen N

Contact person's name, position and contact details: dpo@pleo.io

Activities relevant to the data transferred under these Clauses: Processing necessary to provide the Service pursuant to the Master Service Agreement

Signature and date: This Annex II shall be deemed executed upon execution of the DPA.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

Employees, contractors and consultants engaged by the *Customer Categories of personal data transferred: Name (including first, middle and last name), residential address, telephone number, e-mail address, bank details, billing address, job title, username, employment information, purchase history, expenses history, IP address, and geographic location.Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*
n/a

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

Nature of the processing
Processing necessary to provide the Services pursuant to the Master Service Agreement

Purpose(s) of the data transfer and further processing
Processing necessary to provide the Services pursuant to the Master Service Agreement

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
Until the earliest of (i) expiry/termination of the Master Service Agreement or (ii) the date upon which processing is no longer necessary for the purposes of either party performing its obligations under the Master Service Agreement to the extent applicable).

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
The subject matter, nature and duration of the processing shall be as specified in the Master Service Agreement

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13
In respect of the EU SCCs, means the Danish Data Protection Authority.
In respect of the UK Addendum, means the UK Information Commissioner's Office (ICO).

Annex 2

Technical and organisational measures including technical and organisational measures to ensure the security of the data

EXPLANATORY NOTE:

The technical and organisational 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 organisational 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.

1. **Measures of pseudonymisation and encryption of personal data**

   Pleo maintains Customer Data in an encrypted format at rest.

2. **Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services**

   Pleo commits to strict confidentiality obligations. Additionally, Pleo requires every sub-processor to sign confidentiality provisions.

3. **Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident**

   Pleo performs regular backups of Customer Data, which is hosted in AWS (EU) data centers. Backups are retained across multiple regions and encrypted in transit and at rest using Advanced Encryption Standard.

4. **Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing**

   Pleo maintains a risk-based assessment security program. The framework for Pleo's security program includes administrative, organisational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of Customer Data.

   Pleo's security program is intended to be appropriate to the nature of the Services and the size and complexity of Pleo's business operations.

5. **Measures for user identification and authorisation**

   Pleo employees are required to use unique user access credentials and passwords for authorization. Pleo personnel are authorized to access Customer Data based on their job function, role, responsibilities and seniority. Access is promptly removed upon role change or termination.

6. **Measures for the protection of data during transmission**

   Pleo encrypts data in transit

7. **Measures for the protection of data during storage**

   Credentials are hashed and salted within the services.

8. **Measures for ensuring physical security of locations at which personal data are processed**

Pleo headquarters and office spaces have a physical security program to monitor the overall office security.

The Services operate on Amazon Web Services ("AWS") and Google Cloud ("GCS") and are protected by the security and environmental controls of Amazon and Google, respectively.

Further information about AWS security is available at https://aws.amazon.com/security/ and http://aws.amazon.com/security/sharing-the-security-responsibility/. For AWS SOC Reports, please see https://aws.amazon.com/compliance/soc-faqs/. Detailed information about GCS security is available at https://cloud.google.com/docs/tutorials#security.

9. Measures for ensuring events logging

10. Measures for ensuring system configuration, including default configuration

Pleo relies on infrastructure-as-code processes and internally developed modules to ensure uniform and repeatable systems configuration throughout the infrastructure. Elaborate change management process ensures every change is reviewed by domain experts before a rollout.

Additionally, automated processes are in place to validate adherence to best practices and scan for vulnerabilities or other potential security threats.

11. Measures for internal IT and IT security governance and management

Pleo maintains a risk-based assessment security program. The framework for Pleo's security program includes administrative, organisational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of Customer Data.

Pleo's security program is intended to be appropriate to the nature of the Services and the size and complexity of Pleo's business operations.

Security is managed at the highest levels of the company, with the DPO and Information Security Manager meeting with the Chief Technology Officer regularly to discuss issues and coordinate security initiatives. Information security policies and standards are reviewed and approved by management at least annually and are made available to all Pleo employees for their reference.

12. Measures for certification/assurance of processes and products

Annually, Pleo undergoes third-party assessments/audits for the following standards/certifications: - PCI-DSS (SAQ D) - Google's Cloud Application Security Assessment (CASA) - HackerOne Bug Bounty Penetration Testing - CAIQ Self-Assessment

13. Measures for ensuring data minimisation

Pleo operates under a strict data minimisation principle balanced with the obligations arising from the regulated nature of the service provided.

14. Measures for ensuring data quality

Following processes are used to ensure data quality: dbt Generic Tests and Singular tests, Source Data and Schemas tests, Model logic tests, Integration tests, Dependency check, Code Quality tests, PR review process

15. Measures for ensuring limited data retention

Pleo operates under a strict data retention principle balanced with the obligations arising from the regulated nature of the service provided.

16. Measures for ensuring accountability

Pleo has adopted measures for ensuring accountability, such as implementing Data protection policies across the business, maintaining documentation of processing activities, recording and reporting Security Incidents involving Personal Data, and appointing a Data Protection Officer.

17. Measures for allowing data portability and ensuring erasure

Pleo will provide assistance to the Customer as may reasonably be required under Applicable Data Protection Laws to respond to requests from individuals to exercise their rights under Applicable Data Protection Laws (e.g., rights of data access, rectification, erasure, restriction, portability and objection).

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.

When Pleo engages a sub-processor under this DPA, Pleo and the sub-processor enter into an agreement with data protection terms substantially similar to those contained herein. Each sub-processor agreement must ensure that Pleo is able to meet its obligations to the Customer. In addition to implementing technical and organisational measures to protect personal data, sub-processors must a) notify Pleo in the event of a Security Incident so Pleo may notify the Customer; b) delete data when instructed by Pleo in accordance with the Customer's instructions to Pleo; c) not engage additional sub-processors without authorization; d) not change the location where data is processed; or e) process data in a manner which conflicts with the Customer's instructions to Pleo

SCHEDULE 4
Sub-Processors List

Upon commencement of the DPA, the Controller authorises the engagement of the following sub-processors available in the https://www.pleo.io/en/sub-processors.