

Global Data Processing Addendum

GLOBAL DATA PROCESSING ADDENDUM

This Global Data Processing Addendum (**DPA**) is an addendum to the Agreement between Kainos and Customer and sets forth the obligations of the parties regarding the Processing of Personal Data pursuant to such Agreement.

These [FAQs](#) will assist you with your review of the DPA.

1. DEFINITIONS

Unless otherwise defined below, all capitalized terms have the meaning given within the applicable Agreement.

CCPA	means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., its implementing regulations, and amendments, including the California Privacy Rights Act ("CPRA") and its implementing regulations.
Covered Data	means (i) Customer Data, (ii) any other electronic data or information submitted by or on behalf of Customer to a Covered Service.
Covered Service	means any Workday Service or Subscription Service provided under an Order Form that specifically refers to this DPA.
Customer Data	means such Personal Data which is inputted by the Customer or its Authorized Persons, or retrieved from the Customer's Workday tenant by the Covered Service(s) which is required for the Subscription Service(s) normal operational use.
Data Controller or Controller	means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data, including as applicable any "business" as that term is defined by the CCPA.
DPA	means this Global Data Processing Addendum including any annexures or documents incorporated by reference.
Data Processor or Processor	means the entity which Processes Personal Data on behalf of the Data Controller, including as applicable any "service provider" as that term is defined by the CCPA.
Data Protection Laws	means all data protection laws applicable to the Processing of Personal Data under this DPA, including local, state, national and/or foreign laws, treaties, and/or regulations, including without limitation the GDPR, and implementations of the GDPR into national law, and CCPA in each case as may be amended or superseded from time to time.
Data Subject	means the person to whom the Personal Data relates.
Europe or European	means the European Economic Area ("EEA"), the United Kingdom ("UK") and Switzerland.
GDPR	means either or both the (i) General Data Protection Regulation (EU) 2016/679 ("EU GDPR") and (ii) EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR") as the context may require.
Personal Data	means any Covered Data that relates to an identified or identifiable natural person.
Personal Data Breach	means (i) a 'personal data breach' as defined in the GDPR affecting Personal Data, and (ii) any Security Breach affecting Personal Data.
Processing or Process	means any operation or set of operations performed on Personal Data or sets of Personal Data, such as collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying.
Restricted Country	means: (i) where the EU GDPR applies, a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a country outside the UK which is not based on adequacy regulations pursuant to Section 17A of the UK Data Protection Act 2018 as amended or replaced ("UK DPA"); and (iii) where the Swiss Federal Act on Data Protection of June 19, 1992 as amended or replaced ("Swiss FADP") applies, a country outside Switzerland which has not been recognized to provide an adequate level of protection by the Federal Data Protection and Information Commissioner.
Restricted Transfer	means: (i) where the EU GDPR applies, a transfer of Personal Data from the EEA to a Restricted Country; (ii) where the UK GDPR applies, a transfer of Personal Data from the UK to a Restricted Country; and (iii) where the Swiss FADP applies, a transfer of Personal Data from Switzerland to a Restricted Country.
SCCs	means, as applicable, the EU Standard Contractual Clauses (for any Restricted Transfer subject to the EU GDPR) or the UK Addendum (for any Restricted Transfers subject to the UK GDPR) and any amendment or replacement thereto either (a) pursuant to Data Protection Laws or (b) issued by a competent regulatory authority.
Security Breach	means: (i) any actual or reasonably suspected unauthorized use of, loss of, access to or disclosure of, Customer Data; provided that an incidental disclosure of Customer Data by an Authorized Person or Kainos, or incidental access to Customer Data by an Authorized Person or Kainos, where no reasonable suspicion exists that such disclosure or access involves theft, or is fraudulent, criminal or malicious in nature, shall not be considered a Security Breach for purposes of this definition, unless such incidental disclosure or incidental access triggers a notification obligation under any Law; (ii) Personal Data Breach; and (iii) an security breach (or substantially similar term) as defined by Law affecting Customer Data.
Security Program	means the Relevant Security Program set out in the Agreement.
Sub-processor	means a Kainos Affiliate or third-party entity engaged by Kainos or a Kainos Affiliate as a Data Processor under this DPA, as per the Sub-processor List set out in Annex 1.
Sub-processor List	means the list of Sub-processors included in the Description of Data Processing set out in Annex 1.

2. PROCESSING PERSONAL DATA

Scope and Role of the Parties. This DPA applies to the Processing of Personal Data by Kainos to provide the Covered Service. For the purposes of this DPA, Customer is the Data Controller and Kainos is the Data Processor.

- 2.1. Instructions for Processing. Kainos shall Process Personal Data in accordance with Customer's instructions. Customer instructs Kainos to Process Personal Data to provide the Covered Service in accordance with the Agreement (including this DPA) and as further demonstrated by Customer's use of the Covered Service. Customer may provide additional instructions to Kainos to Process Personal Data, however Kainos shall only be obligated to perform such additional instructions if they are consistent with the terms and scope of the Agreement and this DPA. Where Kainos Processes Personal Information under the CCPA, the terms of the [California Privacy Annex](#) to this DPA will apply to the Processing of such Personal Information.
- 2.2. Compliance with Laws. Kainos will comply with all Data Protection Laws applicable to it in its role as a Data Processor. Customer will comply with all Data Protection Laws applicable to it and shall obtain all necessary consents and provide all necessary notifications to Data Subjects to enable Kainos to carry out data Processing activities. Any instruction issued by Customer to Kainos will comply with applicable Data Protection Laws. Kainos shall inform Customer without undue delay if, in its reasonable opinion, an instruction issued by Customer violates applicable Data Protection Laws.

3. SUB-PROCESSORS

- 3.1. Use of Sub-processors. Customer hereby agrees and provides a general authorization that Kainos and Kainos Affiliates may engage Sub-processors. Kainos or the relevant Kainos Affiliate engaging a Sub-processor will ensure that such Sub-processor enters into a written agreement (with terms no less protective than this DPA) with the Sub-processor that gives effect to the terms set out in this DPA (where applicable). Kainos shall be liable for the acts and omissions of any Subprocessors to the same extent as if the acts or omissions were performed by Kainos.
- 3.2. Sub-processor Objection Right. Customer may object to Kainos' use of a new Sub-processor on reasonable grounds relating to data by providing written notice to Kainos within fourteen (14) days following Kainos' notification pursuant to Section 3.1 above. Should Kainos choose to retain the objected-to Sub-processor, Kainos will notify Customer at least fourteen (14) days before authorizing the Sub-processor to Process Personal Data and Customer may terminate the relevant portion(s) of the Covered Service within thirty (30) days. Upon any termination by Customer pursuant to this section, Kainos shall refund Customer any prepaid fees for the terminated portion(s) of the Covered Service that were to be provided after the effective date of termination.

4. DATA SUBJECT RIGHTS

- 4.1. Assistance with Data Subject Requests. Kainos will, in a manner consistent with the functionality of the Covered Service and Kainos' role as a Data Processor, provide reasonable support to Customer to enable Customer to respond to Data Subject requests to exercise their rights under applicable Data Protection Laws ("**Data Subject Requests**").
- 4.2. Handling of Data Subject Requests. Customer is responsible for responding to Data Subject Requests. If Kainos receives a Data Subject Request or other complaint from a Data Subject regarding the Processing of Personal Data, Kainos will promptly forward such request or complaint to Customer, provided the Data Subject has given sufficient information for Kainos to identify Customer.

5. KAINOS PERSONNEL

Kainos shall require screening of its personnel who may have access to Personal Data, and shall require such personnel (i) to Process Personal Data in accordance with Customer's instructions as set forth in this DPA, (ii) to receive appropriate training on their responsibilities regarding the handling and safeguarding of Personal Data; and (iii) to be subject to confidentiality obligations which survive termination of employment.

6. PERSONAL DATA BREACH

If Kainos becomes aware of a Personal Data Breach, it shall notify Customer within forty-eight (48) hours of becoming aware of such a breach or any shorter period required by Law. Kainos shall take appropriate measures to address and mitigate the adverse effects of the Personal Data Breach. To the extent Customer requires additional information from Kainos to meet its Personal Data Breach notification obligations under applicable Data Protection Laws, Kainos shall provide reasonable assistance to provide such information to Customer taking into account the nature of Processing and the information available to Kainos.

7. SECURITY OF PROCESSING

Kainos shall implement and maintain appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data as described [here](#).

8. AUDIT

Customer agrees that, where applicable, Kainos' then-current SOC 2 audit report (or comparable industry-standard successor reports) and/or Kainos' ISO certifications will be used to satisfy any audit or inspection requests by or on behalf of Customer, and Kainos shall make such reports available to Customer on request. If Customer requires additional information, including information necessary to demonstrate compliance with this DPA, or an audit related to the Covered Service, Kainos will provide reasonable chargeable assistance to the Customer as required to fulfil this requirement, no more than once every 12 months. To the extent that an audit is conducted by a third-party audit firm, (i) the third-party audit firm shall not be a competitor of Kainos and (ii) Customer will, prior to such audit, entered into an agreement with such third-party audit firm containing confidentiality terms no less protective than the confidentiality terms set forth in the Agreement.

9. RETURN AND DELETION OF PERSONAL DATA

Upon termination of the Covered Service, Kainos shall return and delete Personal Data in accordance with the relevant provisions of the Agreement.

10. TRANSFERS OF EUROPEAN PERSONAL DATA

Transfer Safeguards. The transfer safeguards listed below shall apply to all Restricted Transfers:

- 10.1. Processor-to-Processor SCCs. Where Kainos is located within Europe, Kainos has implemented and complies with the SCCs for any Restricted Transfers of Personal Data from Kainos (as "data exporter") to Sub-processors (as "data importers").
- 10.2. Controller-to-Processor SCCs. Where Kainos is located in a Restricted Country, the SCCs will apply to any Restricted Transfers from Customer (as "data exporter") to Kainos (as "data importer") as follows:
 - 10.2.1. EU Personal Data. In relation to Personal Data protected by the EU GDPR, the EU SCCs will apply completed as follows:
 - i. Module 2 applies;
 - ii. in Clause 7, the optional docking clause will apply;

- iii. in Clause 9, Option 2 will apply, the agreed list shall be as per the Description of Data Processing set out in Annex 1 and the specified timeframe will be thirty (30) days;
 - iv. in Clause 11, the optional redress language will not apply;
 - v. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the laws of Ireland;
 - vi. in Clause 18(b), disputes shall be resolved before the courts of Ireland;
 - vii. The details required in Annex I.A can be found in the Agreement; and
 - viii. Annex II of the EU SCCs shall be deemed completed with the Technical and Organisational Measures set out [here](#).
- 10.2.2. UK Personal Data. In relation to Personal Data protected by the UK GDPR ("**UK Personal Data**"), the UK Addendum will apply as follows:
- i. the EU SCCs, completed as set out in Section 10.2.1 above, shall also apply to transfers of UK Personal Data;
 - ii. the UK Addendum shall be deemed executed (and incorporated by this reference) between the transferring Customer and Kainos, and the EU SCCs shall be deemed amended as specified by Part 2 (Mandatory Clauses) of the UK Addendum in respect of the transfer of UK Personal Data;
 - iii. Tables 1 to 3 of the UK Addendum shall be deemed completed with relevant information from within the Agreement and 'option 2' using the EU SCCs, completed as set out in Section 10.2.1 above, shall apply;
 - iv. the start date of the UK Addendum (as set out in Table 1) shall be the effective date of the Agreement; and
 - v. Table 4 of the UK Addendum shall be deemed completed "Importer".
- 10.2.3. Swiss Personal Data. In relation to Personal Data protected by the Swiss FADP, the EU SCCs will apply amended and adapted as follows:
- i. the Swiss Federal Data Protection and Information Commissioner is the exclusive supervisory authority;
 - ii. the term "member state" must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18; and
 - iii. references to the GDPR in the EU SCCs shall also include the reference to the equivalent provisions of the Swiss FADP.
- 11. ADDITIONAL EUROPEAN TERMS**
- 11.1. Description of Data Processing. The agreed subject-matter, the nature, purpose and duration of data processing, the types of Personal Data and categories of Data Subjects are set forth in the Description of Data Processing set out in Annex 1.
- 12. DATA PROTECTION IMPACT ASSESSMENTS ("DPIA(S)") AND PRIOR CONSULTATIONS.**
- Customer agrees that, to the extent applicable, Kainos' then-current SOC 2 audit report (or comparable industry-standard successor reports) and/or Kainos' ISO certifications will be used to carry out Customer's DPIAs and prior consultations, and Kainos shall make such reports available to Customer on request. To the extent Customer requires additional assistance to meet its obligations under applicable Data Protection Laws to carry out a data protection impact assessment and prior consultation with the competent supervisory authority related to Customer's use of the Covered Service, Kainos will, taking into account the nature of Processing and the information available to Kainos, provide reasonable assistance to Customer.
- 13. GENERAL PROVISIONS**
- 13.1. Customer Affiliates. Customer is responsible for coordinating all communication with Kainos on behalf of its Affiliates with regard to this DPA. Customer represents that it is authorized to enter into this DPA and any SCCs entered into under this DPA, issue instructions, and make and receive any communications or notifications in relation to this DPA on behalf of its Affiliates.
- 13.2. Termination. The term of this DPA will end simultaneously and automatically at the later of (i) the termination of the Agreement or, (ii) when all Personal Data is deleted from Kainos' systems.
- 13.3. Conflict. This DPA is subject to the non-conflicting terms of the Agreement. If any inconsistencies between the provisions of this DPA and the Agreement arise, the provisions of this DPA shall prevail with regard to the parties' data protection obligations.
- 13.4. Customer Affiliate Enforcement. Customer's Affiliates may enforce the terms of this DPA directly against Kainos, subject to the following provisions:
- i. Customer will bring any legal action, suit, claim or proceeding which that Affiliate would otherwise have if it were a party to the Agreement (each an "**Affiliate Claim**") directly against Kainos on behalf of such Affiliate, except where the Data Protection Laws to which the relevant Affiliate is subject require that the Affiliate itself bring or be party to such Affiliate Claim; and
 - ii. For the purpose of any Affiliate Claim brought directly against Kainos by Customer on behalf of such Affiliate in accordance with this Section, any losses suffered by the relevant Affiliate may be deemed to be losses suffered by Customer.
- 13.5. Remedies. Customer's remedies (including those of its Affiliates) with respect to any breach by Kainos, its Affiliates and Sub-processors of the applicable terms of this DPA, and the overall aggregate liability of Kainos and its Affiliates arising out of, or in connection with the Agreement (including this DPA) will be subject to any aggregate limitation of liability that has been agreed between the parties under the Agreement.
- 13.6. Miscellaneous. The section headings contained in this DPA are for reference purposes only and shall not in any way affect the meaning or interpretation of this DPA.

ANNEX 1:

[Description of Data Processing](#)