Data Processing Addendum ("DPA")

This Data Processing agreement (DPA) forms part of the agreement between Client and Unisys (Client Agreement) under which Unisys agrees to provide Client with certain products and services. To the extent Unisys may be required to process personal data on behalf of Client under the Client Agreement or Order, Unisys will do so under the terms set out in this DPA.

1. Definitions

1.1. **"CCPA"** means the California Consumer Privacy Act of 2018, as amended (Cal. Civ. Code §§ 1798.100 to 1798.199); specific processing terms are set out in **Attachment E.**

1.2. **Client Agreement:** means the agreement between Client and Unisys, whether under a written order from Client for the products or services (A) directly with Unisys that is accepted by Unisys, or (B) with a Unisys reseller, subject to Unisys acceptance of an order for the Services from its reseller (the "Order").

1.3. "**Data Controller**": means the party/entity which, alone of jointly with others, determines the purposes and means of the Processing of Personal Data.

1.4. **"Data Exporter"** means a party that is transferring Personal Data directly or via onward transfer to a Restricted country .

1.5. "**Data Importer**" means a party that receives Personal Data directly from a Data Exporter, or via onward transfer and that is located in a Restricted country.

1.6. "**Data 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.

1.7. "**Data Protection Laws"** means all data protection laws applicable to the Processing of Personal Data processed under this DPA; including but not limited to (each as amended or replaced from time to time) (a) EU Data Protection Laws, (b) UK Data Protection Laws, (c) the CCPA, (d) the Swiss Federal Act of 19 June 1992 on Data Protection ('**FADP**'), and (e) any equivalent national laws or regulations once in force and applicable and in each case as amended, superseded or replaced from time to time.

1.8. **"Data Subject":** means the natural person to whom Personal Data relates or legal person (to the extent data of a legal person are protected similarly as data of natural persons under applicable Data Protection Laws).

1.9. "**EEA":** means the European Economic Area.

1.10. "**EU Data Protection law" or "GDPR":** means the General Data Protection Regulation (EU2016/679)

1.11. "**EU SCCs":** shall mean Sections I, II, III and IV (as applicable) in so far as they relate to Module Two (Controller-to-Processor) and Module Three (Processor-to-Processor) as applicable, within the Standard Contractual Clauses for the transfer of Personal Data to third countries under Regulation (EU) 2016/679 of the European Parliament and the Council approved by EC Commission Decision of 4 June 2021, as set out in **Attachment C**.

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

1.13. "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

1.14. "**Process" or "Processed" or "Processing**" shall have the meaning have the meaning given to them in applicable Data Protection Laws, or if not defined therein the GDPR and the terms "Business" and "Service Provider" have the meanings given to them in the CCPA.

1.15. **"Sub-processor"**: means a Unisys Affiliate or third party entity engaged by Unisys which may Process Personal Data as a Data Processor as instructed by Unisys.

1.16. **"Sub-processor list":** means the Sub-processor list identifying the Sub-processors that are authorized to Process Personal Data accessible through Unisys website.

1.17. **"Regulator"**: Supervisory Authority, Data Protection Authority or equivalent term under Applicable Data Protection Law.

1.18. "**Restricted Country":** means (1) where the GDPR applies, a country outside 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 so June 19, 1992 as amended or replaced ("Swiss ADP") applies a country outside Switzerland which has not been recognized to provide an adequate level of protection the Federal Data Protection and Information Commissioner.

1.19. **"Restricted Transfer"**: means a transfer of Personal Data from a Data Exporter to a Data Importer; where the GDPR applies a transfer from the EEA to a Restricted Country (ii) where the UK GDPR applies a transfer from the UK to a Restricted Country and (iii) where the Swiss FADP applies a transfer from Switzerland to a Restricted Country.

1.20. **"Services"** shall mean the services provided or to be provided by Unisys to Client under the Client Agreement.

1.21. "**Standard Contractual Clauses"** or "**SCCs"** means any pre-approved standard contractual clauses for the international transfer of personal data under applicable Data Protection Laws, including the EU SCCs, the Swiss Addendum (the EU SCCs as amended by **Attachment D**) and UK Addendum, as may be updated, supplemented, or replaced from time to time under applicable Data Protection Laws, as a recognized transfer or processing mechanism (as applicable).

1.22. **"UK Addendum":** means *the International Data Transfer Addendum* issued by the Information Commissioner's Office in accordance with UK Data Protection Law as issued by the ICO available at; international-data-transfer-agreement.pdf (ico.org.uk); international-data-transfer-addendum.pdf (ico.org.uk) and set out in **Attachment D**

1.23. '**UK Data Protection laws**' means the GDPR as implemented in the UK.

2. Compliance with Laws, Data Ownership of Personal Data

2.1. As between the parties, all Client Data remains, at all times, the property of Client and Client shall have sole responsibility for the accuracy, quality and legality of Personal Data it provides to Unisys. Client remains responsible for its compliance obligations under applicable Data Protection Laws, including providing any required notices to Data Subjects, obtaining any required consents and providing notifications to Regulators. Unisys is responsible for compliance with its respective obligations as Data Processor under this DPA and applicable Data Protection Laws.

2.2. The parties agree and acknowledge that their factual circumstances dictate their respective designation as a Data Controller or Data Processor. Notwithstanding the foregoing the parties agree that for the purpose of this DPA, Client and its Affiliates are the Data Controller(s) and Unisys and its Affiliates are the Data Processor. Unisys will process Personal Data solely to perform the Services in accordance with the Client Agreement.

3. Scope of processing and instruction rights of the Controller

3.1. This DPA are meant to be Client's original instructions to Unisys for the Processing of Personal Data; Client may issue additional instructions in writing taking into account the nature and purpose of Unisys services. Client as Data Controller shall ensure that any instruction it issues to Unisys complies with applicable Data Protection Laws to enable Unisys to carry out lawfully the Processing contemplated under the DPA. Unisys shall inform client without undue delay if, in its reasonable opinion, an instruction issued by Client violates applicable EU Data Protection Law.

3.2. Subject to Unisys complying with its obligation under clause b) in 4.1 below, Client will respond to all requests made by Data Subjects under applicable Data Protection Laws and all communications from and to Regulators which relate to Personal Data Processed by Unisys for Client under this DPA.

4. Obligations of the Processor

4.1. When Processing Personal Data in its capacity as a Processor, Unisys will:

a) process the Personal Data in accordance with Client instructions; the agreed subject matter, the nature, purpose and duration of the Processing the categories of Personal Data and categories of Data Subjects are set forth in **Section A, "Processing Details".**

b) inform Client if Unisys has received a request or complaint from any Data Subject with a request for exercising his or her rights ("**Data Subject Request -DSR**") in relation to the Personal Data processed by Unisys, provided the Data Subject has given sufficient information to Unisys. To the extent Client is not able to respond to such DSR without Unisys support, Unisys will provide reasonable assistance taking into account the type of services Unisys provides under the DPA. For the avoidance of doubt, Client is responsible for timely responding to DSR's.

c) use commercially reasonable efforts to assist Client to comply with its obligations under applicable Data Protection Laws such as breach notifications, Data Protection Impact Assessments and if necessary consultation with Supervisory Authorities provided Client shall pay Unisys' reasonable charges for providing the assistance.

d) provide that persons authorized to process the Personal Data have the necessary professional skills and competence to perform such activities, have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and undertake the annual training on their responsibilities regarding the handling and safeguarding of Personal Data.

e) to the extent required under Data Protection Law keep records of Processing which Unisys carries out for Client, which will include the information required to be kept and provide Client with a copy of those records on request;

f) implement appropriate technical and organizational measures to protect the Personal Data from the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data transmitted, stored or otherwise Processed. Unisys may update or modify these measures from time to time provided that such updates and modifications do not result in a degradation to the overall level of security. These T&O measures are summarized in **attachment B**; upon request Unisys will provide the full description of T&O measures.

5. Return and deletion of Client Personal Data

5.1. Upon expiration or termination of the provision of the Services pursuant to the Client Agreement and subject to clause 5.2 below, Unisys will securely destroy all Personal Data including any copies thereof held in its possession and/or control, and on request send Client a written certification that all Personal Data has been so destroyed or return the Personal Data in the format it was stored by Unisys.

5.2. If Unisys is required to retain Personal Data in order to comply with applicable laws, then Unisys may retain the Personal Data, and will retain it in compliance with applicable Data Protection Laws and not Process the Personal Data except for the purpose of complying with applicable laws.

6. Personal Data Breach and Response

6.1. Unisys will notify Client's point of contact as detailed in the Client Agreement without undue delay after becoming aware of a Personal Data Breach and provide reasonable cooperation and assistance in order for Client to meet its data breach reporting obligations under applicable Data Protection Laws taking into account the nature of Processing and the information available to Unisys. Unisys shall take appropriate measures to address and mitigate the adverse effects of the Personal Data breach.

6.2. Except as required by applicable Data Protection Laws, Unisys agrees that: (i) it shall not inform any third party of any Personal Data Breach without first obtaining Client's prior written consent, other than to inform a complainant that Client shall be/has been informed of the Personal Data Breach; and (ii) Client shall have the sole right to determine whether notice of the Personal Data Breach is to be provided to any individuals, Regulators, law enforcement agencies, consumer reporting agencies, or others and the contents of the notice.

6.3. Client will not communicate or publish any notice or admission of liability concerning a breach which directly or indirectly identifies Unisys without Unisys prior approval, unless Client is compelled to do so under applicable Data Protection Law. In any event Client shall provide Unisys with reasonable prior written notice of any such communication or publication.

7. Appointment of Sub-processors

7.1. Client hereby provides general written authorization that Unisys and its Affiliates may engage Sub-processors to process Personal Data. Unisys shall make available to Client a Sub-processor list. At least thirty (30) days prior to authorizing any new Sub-processor Unisys shall provide notice to Client by updating the Sub-processor list.

7.2. Unisys or the relevant Unisys Affiliate engaging a third party Sub-processor shall ensure that such Sub-processor has entered into a written agreement that is no less protective than this DPA. Unisys is responsible for the performance of its Sub-processors in compliance with the terms of this DPA and Applicable Data Protection Laws and Unisys shall be liable for the acts and omissions of any of its Sub-processors.

8. Sub-processor Objection right. This Section 8 shall apply only where and to the extent Client is established in Europe, UK or Switzerland or where otherwise required by applicable Data Protection Laws. Unisys will inform Client of any addition, removal or replacement of the sub-processor(s). Within fourteen (14) calendar days of Unisys providing Client notice of the change, Client may object to the involvement of a new proposed Sub Processor, providing objective justifiable grounds related to the ability of such sub-processor to adequately protect Personal Data according to the DPA or applicable Data Protection Laws in writing to the Unisys. Unisys and Client will work together in good faith to find a mutually acceptable resolution to address such objection. To the extent Client and Unisys do not reach a mutually acceptable resolution within a reasonable timeframe, Client may terminate the relevant Services (i) upon serving thirty (30) days prior written notice to Unisys; (ii) without liability to Client or Unisys and (iii) without relieving Client from payment obligations up to the date of termination **Restricted Transfers**

8.1 Without prejudice to any applicable regional data center restrictions for some type of Services specified in the Client Agreement , Unisys may Process Personal Data globally as necessary to perform the Services. Unisys relies of appropriate statutory transfer mechanisms for international data transfers and has appropriate agreements in place to support cross-border transfers of Personal Data.

8.2 Where there is a Restricted Transfer of Personal Data, the Data Exporter and the Data Importer must transfer and process the Personal Data under applicable Data Protection Law in particular:

8.2.1 **Attachment C** will apply where Personal Data subject to EU Data protections Law is transferred from a Data Exporter to a Data Importer acting as a Processor

8.2.2 **Attachment D** will apply where Personal Data that is subject to applicable Data Protection Laws in the specific jurisdiction provisions.

8.3 **Execution of SCCs**. If any cross-border transfer of Personal Data between Client and Unisys requires the execution of SCCs to comply with the applicable Data Protection Law, the parties' signature to this DPA or to any other binding document which otherwise incorporates the DPA will be considered as signature to the SCCs by the terms set out therein.

8.4 **Change of statutory transfer mechanism**. To the extent that parties are relying on the EU SCCs or another specific statutory mechanism to normalize international data transfers and those mechanisms are subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, parties agree to cooperate in good faith to promptly suspend the transfer or to pursue a suitable alternate mechanism that can lawfully support the transfer.

9. Audit rights

9.1 Client acknowledges that Unisys' managed digital service centers and data centers are certified to ISO standards, including ISO 9001, ISO 20000, ISO 27001 and ISO 22301. Unisys conducts annual internal security assessments and facilitate external independent verification and validation audits to maintain these certifications. SSAE SOC 1 Type II audits of all major digital service centers and data centers are performed each year. More information on Unisys Information Security and Data policies and procedures can be found here: https://www.unisys.com/brochure/privacy-secured/

9.2 Client agrees that, to the extent applicable, Unisys audit reports and/or Unisys ISO certifications will be used to satisfy any audit or inspection requests by or on behalf of Client. Upon reasonable notice Unisys shall make a (summary) copy of its audit report(s) available to Client, which reports shall be subject to the confidentiality provisions of the Client Agreement. If Client requires additional information, including information necessary to demonstrate compliance with this DPA or an audit related to the Services, Unisys will provide Client with reasonable assistance and respond to any written audit questions to demonstrate compliance with its obligations as a Processor under applicable Data Protection Laws. Client will not exercise this right more than once a year.

10. General provisions

10.1 Unisys has implemented measures to regulate the disclosure of Client Data to a government entity. These measures require Unisys to consider its obligations to comply with any order or demand and any legal obligations to protect our customer's Personal Data or Confidential Information. With regard to data of EU. UK and Swiss residents, Unisys abides by the obligations set forth in any legal mechanism relied on for data transfers to third countries, such as the SCC's and UK Addendum. Specifically, to the extent permitted by law, Unisys will promptly notify the Client of the order or demand before Unisys will respond. If Unisys is not permitted to provide notification to the Client, Unisys will seek permission to notify the Client or ask the issuing court or government authority to seek the requested documents directly from the Client. Unisys will challenge an order or demand when appropriate and valid legal grounds exist. If Unisys is required to comply with a valid Court order or demand, Unisys will disclose the minimum amount of Client Personal Data or Confidential Information necessary to comply.

11. General provisions

11.1. **Affiliates**: To the extent applicable each party is entering into this DPA also on behalf of its Affiliates. Each party will coordinate all communication with the other party on behalf of its Affiliates with regard to this DPA. Client represents that it is authorized to issue instructions and make and receive any communications or notifications relating to this DPA on behalf of its Affiliates. Either party's Affiliates may enforce the terms of the DPA directly against the other party subject to the following provisions: (i) each party will bring any legal action, suit, claim or proceeding which that Affiliate would otherwise have if it were a party to the Order (each an Affiliate Claim) directly against the other party on behalf of the Affiliate, except where the applicable Data Protection Laws or other applicable laws to which the relevant Affiliate is subject require that the Affiliate itself bring or be party to the Affiliate Claim and (ii) for the purpose of any Affiliate Claim brought directly against one party by the other on behalf of its Affiliate according to this Section, any losses suffered by the relevant Affiliate may be deemed to be losses suffered by the party bringing the claim. If needed for local legal reasons the parties will enter into a local DPA with their relevant local Affiliates.

11.2. **Remedies:** Client's remedies (including those of its Affiliates) with respect to any breach by Unisys, its Affiliates and Subprocessors of the applicable terms of this DPA and the overall aggregate liability of Unisys and its Affiliates arising out of, or in connection with the Client Agreement including this DPA will be subject to any aggregate limitation of liability that has been agreed between the parties under the Client Agreement.

11.3. **Conflict.** This DPA is subject to the non conflicting terms of the Client Agreement. With regard to the subject matter of this DPA if inconsistencies between the provision of this DPA and the Client Agreement arise, the provisions of this DPA shall prevail with regard to the parties' data protection obligations.

11.4. **Miscellaneous.** The section headings contained in this DPA are for reference purposes only and shall not in any way affect the meaning of interpretation of this DPA.

11.5. **Governing law**. This DPA is governed by the laws of the country specified in the relevant provisions of the Client Agreement and the EU SCCs and UK Addendum are governed by the laws as provided for in the EU SCCs or UK Addendum.

11.6. **Termination:** The term of this DPA will end simultaneously and automatically at the later of (i) the termination of the Client Agreement or (ii) when all Processing activities under the DPA have ended.

Attachment A: Processing Details

Client and Unisys acknowledge and agree that depending on Client's use/receipt of the Services:

a) The **purpose of the processing and data transfer** shall be to provide the Services according to the Client Agreement; additional or more specific descriptions of Processing activities, categories of Personal Data and Data Subjects may be described in the Client Agreement or, for Unisys standard commercial Service offerings, at the site where Client and its Authorized Users access the Services, Unisys support site at https://public.support.unisys.com/common/ShowWebPage.aspx?id=8143&pla=ps&nav=ps or other Unisys URL identified by Unisys in the Order (**"Unisys Site"**)..

b) The **categories of Personal Data transferred** may include but are not limited to basic personal data (*for example first and last name, email address, home and work address*), contact information (*for example work email and phone number*), authentication data (*for example username and password*), bank account information, identification numbers (*for example IP addresses*), professional or employment-related information (for example, employer name and job title); educational information (*for example certifications, work history and qualifications)*, location data and device identification.

c) The **categories of data subjects** can be Client's representatives and end users, including its employees, job applicants, contractors, partners, suppliers, clients and customers;

d) The **nature of processing** can be **(1) receiving data** (including collection, accessing, retrieval, recording, and data entry), (2) **holding data** (including storage, organisation and structuring, (3) **using data** (including analysing, consultation, testing, automated decision making and profiling), (4) **updating data** (including correcting, adaptation, alteration, alignment and combination), (5) **protecting data** (including restricting, encrypting, and security testing), (6) **sharing data** (including disclosure, dissemination, allowing access or otherwise making available, (7) **returning data** to the data exporter or data subject or (8) **erasing data**, including destruction and deletion

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

See clause 5 of the DPA

f) **Points of Contact**: As between Client and Unisys, Client is the Data Controller and Data Controller details are in Client Agreement; the contact information of the Data Processor for the DPA is: **unisysglobalprivacy@unisys.com.**

Attachment B: Technical and Organizational Measures summary

As a Data Processor, Unisys shall:

a) Ensure that the Personal Data can be accessed only by authorized personnel for the purpose of processing;

b) Take all reasonable measures to prevent unauthorized access to Personal Data through the use of appropriate physical and logical (passwords), entry controls, securing areas for data processing, and implementing procedures for monitoring the use of data processing facilities;

c) Build in system and audit trails;

d) Use secure passwords, network intrusion detection technology, encryption and authentication technology, secure logon procedures and virus protection;

e) Account for risks that are presented by processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorized or unlawful storage, processing, access or disclosure of Personal Data;

f) Ensure pseudonymisation and/or encryption of Personal Data when appropriate;

g) Maintain the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

h) Maintain the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

i) Implement a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing of Personal Data;

j) Monitor compliance on an ongoing basis;

k) Implement measures to identify vulnerabilities with regard to the processing of Personal Data in systems used to provide services to the Data Controller; and,

l) Provide employee and contractor training to ensure ongoing capabilities to carry out the security measures established in policy.

Additional or more specific Technical and Organizational Measures for the specific Services may be described in the Client Agreement or, for Unisys standard commercial Service offerings, at the Unisys Site.

Attachment C – EU standard contractual clauses

1 Definitions

For the purposes of this **Attachment C**, the following definitions will apply:

'**C-to-P Transfer Clauses**' means Module Two (Controller-to-Processor) within the Standard Contractual Clauses for the transfer of Personal Data to third countries which Module will apply insofar the transfer relates to Personal Data which the Data Exporter transfers in its capacity as Controller.

'**P-to-P Transfer Clauses**' means Module Three (Processor-to-Processor) within the Standard Contractual Clauses for the transfer of Personal Data to third countries and will apply insofar the transfer relates to Personal Data which the Data Exporter transfers in its capacity as Processor. Where Unisys acts as Data Exporter Client acknowledges and agrees that Unisys can rely on its Intragroup Data processing and data transfer agreement incorporating the P-to-P model clauses.

The SCC's are hereby incorporated into this DPA by reference and shall apply in full subject to the below terms:

Where the EU SCC's identify option provisions (or provisions with multiple options) the following applies:

(a) Section 7 (docking clause) of the EU SCCs will apply

(b) In Section 9 (a) use of sub-processors – Option 2 is elected (general written authorization; specified time-period 30 days). The parties shall follow the process and timings agreed in clause 7 of the DPA.

(c) In Section 11(a) (Redress) – the optional provision will not apply

(d) In Section 17 (Governing Law) – Option 2 shall apply and where such law does not allow for third party beneficiary rights the parties agree that this shall be the law of the Netherlands; and

(e) In Section 18 (b) (Choice of forum and jurisdiction) – the Courts of the country where the Data Exporter is established shall have jurisdiction.

Annex I-A (List of the Parties): reference is made to the parties listed in the Client Agreement; **Attachment A** includes the contact person's name, position and contact details. The parties agree that their signature to the Client Agreement/this DPA or other binding document which otherwise incorporates the DPA will be considered as signature to the SCCs in accordance with the terms set out therein.

Annex I B The processing activities relevant to the transfer of Personal Data under the EU SCCs relate to the provision/ reception of the Services by Client/Unisys under the Client Agreement and Personal Data, nature of processing, data subjects are further detailed in **Attachment A** above. The frequency of the transfer (e.g. whether the date is transferred on a one-off or continuous basis): continuous for the duration of the Agreement unless specifically addressed as one-off in the Agreement.

Annex I C SCC's: Competent Supervisory Authority: Where the data exporter is established in the EU, the supervisory authority in the country of the establishment of the data exporter. A full list of EU supervisory authorities can be found here https://edpb.europa.eu/about-edpb/about-edpb/members_en. In any other cases the supervisory authority is the authority competent in the Netherlands

Annex II SCC's - Technical and Organisational Measures of the SCCs shall be deemed completed with the terms as set out in **Attachment B** of the DPA.

Annex III SCC's- List of Subprocessors as set out in the Client Agreement and Sub-processor list.

2. SUPPLEMENTARY TERMS TO EU SCCs.

(a) COMMUNICATION. The Parties agree that all notices, requests, monitoring rights required under the EU SCCs shall be provided, as applicable, to the Unisys entity that is a party/signatory to the Client Agreement.

(b) ERASURE OR RETURN OF DATA: for the purposes of Section 8.5 Data Importer shall delete or return personal data in accordance with the deletion provisions set out in the DPA. For the purposes of clause 16 (d) the deletion provisions set out in clause 5 of the DPA shall also apply.

(c) DOCUMENTATION AND COMPLIANCE. For the purposes of Section 8.9 of the EU SCC's the review and audit provisions in clause 9 of the DPA shall primarily apply. To the extent Data Exporter's audit requirements under the SCC's or Data Protection Requirements cannot reasonably be satisfied through the reports, documentation or compliance information Unisys generally makes available to its customers, Unisys will respond to Client's reasonable additional audit instructions.

Attachment D – Other EU jurisdictions

Switzerland

Where a Restricted Transfer of Personal Data from a Data Exporter to a Data Importer is subject to the GDPR and the FADP, the following additional provisions to the EU SCCs will apply for the EU SCCs to be suitable for ensuring an adequate level of protection for such transfer in accordance with Article 6 paragraph 2 letter (a) of FADP:

(a) '**FDPIC**' means the Swiss Federal Data Protection and Information Commissioner.
(b) '**Revised FADP**' means the revised version of the FADP of 25 September 2020, which is scheduled to come into force on 1 January 2023.
(c) The term '**EU Member State**' must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility for pursuing their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c).
(d) The EU SCCs also protect the data of legal entities until the entry into force of the Revised FADP.
(e) The FDPIC will act as the 'competent supervisory authority' insofar as the relevant Restricted Transfer is governed by the FADP.

UK (the United Kingdom of Great Britain and Northern Ireland)

Where a Restricted Transfer of Personal Data from a Data Exporter to a Data Importer is subject to UK Data Protection Laws, this section of Attachment D will apply.

PART 1: TABLES

Table 1: Parties

Start date	**Data of the execution of the Client Agreement**	
The Parties	**Data Exporters** (who sends the Restricted Transfer)	**Data Importer** (who receives the Restricted Transfer)
Parties' details	Client name as set out in the Client Agreement where Client acts as data Exporter Or Unisys UK where Unisys UK acts as Data Exporter	Full legal name: Unisys Corporation Trading name (if different): UIS/Unisys Main address (if a company registered address): 801 Lakeview Drive Suite 100, Blue Bell, PA 19422 Official registration number (if any) (company number or similar identifier): N/A
Key Contact	Please see Attachment A	Chief Privacy Officer; unisysglobalprivacy@unisys.com
Signature (if required for the purposes of Section 2): N/A		N/A

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to, see **Attachment C**, including the Appendix Information:

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:

a) Annex 1A: List of Parties: see table I

b) Annex 1B: Description of Transfer: see **Attachment A**

c) Annex II: Technical and Organisational measures to ensure the security of the data: see **Attachment B**

d) Annex III: List of Sub-processors (Modules 2 and 3 only): see **Attachment C**

Table 4: Ending this Addendum when the Approved Addendum Changes

e) **Ending this Addendum when the Approved Addendum changes**	f) Which Parties may end this Addendum as set out in Section 19: g) x Importer h) x Exporter i) ☐ Neither Party

PART 2 – MANDATORY CLAUSES

Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 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 of those Mandatory Clauses.

Attachment E: California Consumer Privacy Act Terms

These CCPA/CPRA terms only apply where Unisys processes personal data of California residents.

1 Definitions

1.1 The following definitions apply:
"CCPA" means the California Consumer Privacy Act of 2018, as amended (Cal. Civ. Code §§ 1798.100 to 1798.199), and any related regulations or guidance provided by the California Attorney General.
"Contracted Business Purposes" mean the purposes for processing personal information as set out in **Attachment A**.
"Personal Information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

1.2 The following lower case terms used but not defined in this **Attachment E**, such as 'aggregate consumer information', 'business purposes', 'commercial purposes', 'consumer', 'de-identify', 'processing', 'pseudonymize', 'sale', and 'verifiable consumer request' will have the same meaning as set forth in §§ 1798.14 of the CCPA.

2. Unisys CCPA Obligations

2.1 Unisys will only process Personal Information for the Contracted Business Purposes for which Client provides or permits Personal Information access, including under any 'sale' exemption.

2.2 Unisys will not process, sell, or otherwise make Personal Information available for Unisys' own commercial purposes or in a way that does not comply with the CCPA. If a law requires Unisys to disclose Personal Information for a purpose unrelated to the Contracted Business Purposes, Unisys must first inform Client of the legal requirement and give Client an opportunity to object or challenge the requirement, unless the law prohibits such notice.

2.3 Unisys will limit Personal Information processing to activities reasonably necessary and proportionate to achieve the Contracted Business Purposes or another compatible business purpose.

2.4 Unisys will comply with any Client request or instruction from Authorized Persons requiring Unisys to provide, amend, transfer, or delete the Personal Information, or to stop, mitigate, or remedy any unauthorized processing.

2.5 If the Contracted Business Purposes require the collection of Personal Information from consumers on Client's behalf, Client must provide Unisys with a CCPA-compliant notice addressing use and collection methods that Client specifically pre-approves in writing. Unisys will not modify or alter the notice in any way without Clients prior written consent.

2.6 If the CCPA permits, Unisys may aggregate, de-identify, or anonymize Personal Information so it no longer meets the Personal Information definition, and may use such aggregated, deidentified, or anonymized data for its own research and development purposes.

3 Assistance with Clients CCPA Obligations

3.1 Unisys will reasonably cooperate and assist Client with meeting Clients CCPA compliance obligations and responding to CCPA-related inquiries, including responding to verifiable consumer requests, taking into account the nature of Supplier's processing and the information available to Supplier.

3.2 Unisys will notify Client immediately if it receives any complaint, notice, or communication that directly or indirectly relates to either party's compliance with the CCPA. Specifically, Unisys will notify Client within 5 working days if it receives a verifiable consumer request under the CCPA.

4 Subcontracting

4.1 Unisys may use subcontractors to provide the Contracted Business Purposes. Any subcontractor used must qualify as a service provider under the CCPA and Unisys will not make any disclosures to the subcontractor that the CCPA would treat as a sale.

4.2 For each subcontractor used, Unisys will give Client an up-to-date list disclosing:
(a) The subcontractor's name, address, and contact information.
(b) The type of services provided by the subcontractor.
(c) The Personal Information categories disclosed to the subcontractor in the preceding 12 months.

4.3 Unisys remains fully liable to Client for the subcontractor's performance of its agreement obligations. Unisys will audit a subcontractor's compliance with its Personal Information obligations on a periodic basis and provide Client with the audit results on request.

5 CCPA Warranties

5.1 Both parties will comply with all applicable requirements of the CCPA when processing Personal Information.

5.2 Unisys warrants that it has no reason to believe any CCPA requirements or restrictions prevent it from providing any of the Contracted Business Purposes or otherwise performing under this DPA. Unisys will promptly notify Client of any changes to the CCPA's requirements that may adversely affect its performance under the DPA.

INTENTIONALLY LEFT BLANK