UNISYS | Securing Your Tomorrow®

Data Privacy Addendum ("DPA") To

_____ (the "Agreement") Dated as of _____

Between Unisys <entity name, address, location> ("Unisys") and _____ ("Supplier")

This DPA shall, effective as of the date executed below, be incorporated into and form part of the Agreement between Unisys and Supplier, under which Agreement Supplier provides the agreed Services *to Unisys*. Terms not defined herein (including in Annex I: Definitions) shall have the meaning set forth in the Agreement. In the event of a conflict between the DPA and Agreement, the terms and conditions of the DPA shall prevail with regard to the parties' data protection obligations.

All Unisys Data (defined below) shall be deemed "Confidential Information" under the Agreement. The parties' confidentiality obligations under this DPA shall survive five years after the termination or expiration of the Agreement, except that Personal Data must be treated as Confidential Information in perpetuity.

1. Compliance with Laws, Data Ownership of Personal Data

1.1 Supplier shall comply with all Data Protection laws applicable to Supplier in connection with the provision of the Services and Unisys shall comply with all Data Protection Laws applicable to Unisys in connection with its receipt of the Services.

1.2 As between the parties, all Unisys Data remains, at all times, the property of Unisys.

1.3 Unisys hereby informs Supplier that if in connection with the Agreement Unisys receives Personal Data from the Supplier, Unisys will Process such Personal Data is accordance with the "Unisys Privacy Notice", which is available at http://www.unisys.com/unisys-legal/privacy and incorporated herein by reference.

2. Supplier's Obligations

2.1 For the purposes of this DPA:

a) other than Unisys Data for which Unisys's clients are Data Controllers, Unisys and its Affiliates shall be the Data Controllers of Unisys Data; and

b) Unisys and its Affiliates shall be Data Processors of Unisys Data for which Unisys' clients are Data Controllers; and

c) Supplier shall be a Data Processor of Unisys Data where Unisys is a Data Controller of that data and a Subprocessor of Unisys Data where Unisys is a Data Processor of that data.

2.2 Supplier shall Process Personal Data in accordance with Unisys documented instructions as set out in the Agreement and Annex II. Unisys may provide additional instructions to Supplier to Process Personal Data. Supplier shall not process the Personal Data for any other purpose, including but not limited to marketing Supplier's products or services, unless specifically instructed by Unisys in writing. For the avoidance of doubt, Supplier is prohibited from selling, renting, releasing, disclosing, disseminating, making available, transferring or otherwise communicating orally, or in writing, or by electronic or other means Personal Data to another entity (whether affiliated or not), except as expressly permitted by the DPA or the Agreement. Supplier certifies that it understands and will comply, and cause all Supplier personnel to certify that they understand and will comply with the requirements of this DPA. Supplier shall immediately inform Unisys if it cannot comply with an instruction or, in its opinion, an instruction infringes applicable Data Protection laws.

2.3 To the extent Supplier is authorized by Unisys to collect Personal Data directly from individuals in connection with the provision of the Services under the Agreement, Supplier shall provide a privacy notice in an intelligible and easily accessible form, using clear and plain language and obtain explicit consent, if required, in accordance with applicable laws. The notice, at a minimum, should describe the purpose of the collection, intended use, disclosure of collected Personal Data, how the Personal Data will be protected, and the right to withdraw consent, if consent is the basis for Processing.

2.4 Supplier shall encrypt Highly Restricted Data at all times, including at time of collection, and during use, transmission and storage.

2.5 Supplier shall maintain records of Processing activities, including, but not limited to:

a) the name and contact details of the Supplier and any other subcontractors and, where applicable, of the Unisys' or Supplier's representative, and the data protection officer;

b) the categories of Processing carried out on behalf of Unisys;

c) where applicable, information on cross-border transfers, including transfers of Personal Data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers outside of the legally specified transfer mechanisms, the documentation of suitable safeguards for the Personal Data;

d) a general description of the technical and organizational measures. Supplier agrees to make such records of Processing available upon request to Unisys and regulators.

2.6 The records referred to above shall be in writing, including in electronic form. Supplier shall provide the records and additional information about Supplier and its Processing of Unisys Data as reasonably requested by Unisys for the purpose of assisting Unisys and Unisys clients (where Supplier acts as a Subprocessor and Unisys as a Data Processor) in complying with Unisys' and relevant client's (as applicable) obligations under applicable Data Protection laws or contracts, including the exercise of data subject rights, data protection impact assessments, prior consultation and Personal Data Breach notification obligations as well as investigations and as necessary for Unisys and relevant clients (as applicable) to demonstrate compliance with applicable Data Protection Laws.

2.7 Supplier shall assist Unisys and Unisys clients (where Supplier acts as a Subprocessor and Unisys as a Data Processor) to allow Unisys and Unisys client (as appropriate) to comply with their respective obligations under applicable Data Protection laws, including, but not limited to, responding to Data Subjects' rights, data protection impact assessments, prior consultation, security and security breach notification as well as investigations. Supplier shall also allow Unisys and Unisys clients, upon reasonable advance written notice, to check and audit its data processing facilities, procedures and records, either itself or through a third independent contractor at Unisys' or client's (as appropriate) expense, in order to ascertain compliance with Data Protection Laws and the terms of this DPA, the Agreement and the agreement between Unisys and the client (where Supplier acts a Subprocessor under the terms of this DPA). Supplier and its personnel shall fully cooperate with reasonable audit requests by providing access to relevant knowledgeable personnel, physical premises, documentation, infrastructure and application software. In addition, Supplier will provide, at no cost to Unisys or client (as applicable), copies of any routine or other Service Organizational Control (SOC) reports, including SOC 1, Type 2, and SOC 2 reports or equivalent and other data security or data protection related audits, as applicable to the Services. After conducting an audit, Unisys will notify Supplier of any non-compliance. Upon such notice, Supplier shall promptly take the necessary measures to remedy such non-compliance. Unisys is allowed to share all audit results and documentation provided by Supplier to Unisys to the Controller (Client) where Unisys is the Processor under the contract.

2.8 Supplier shall provide Unisys with the name and contact details of its Data Protection Officer if it has appointed one or otherwise another person who is responsible for data protection compliance within Supplier's organization.

2.9 Unisys is responsible for responding to Data Subject Requests for access, correction, deletion or restriction of that person's Personal Data ("**Data Subject Request**"). If Supplier receives a Data Subject Request, Supplier shall promptly redirect the Data Subject Request to Unisys and enable Unisys to meet its obligations under applicable Data Protection Laws by providing reasonable cooperation and assistance in responding to the Data Subject.

2.10 Should any court, government agency or law enforcement agency contact Supplier with a demand for Unisys Data, Supplier will direct the law enforcement agency to request such information directly from Unisys. As part of this effort, Service Provider may provide Unisys's basic contact information to the agency. If compelled to disclose Unisys Data to law enforcement or any government agency, then Supplier will promptly, and without any undue delay, notify Unisys and deliver a copy of the request (except in such cases in which Supplier is specifically legally prohibited from doing so) to allow Unisys to seek a protective order or any other appropriate remedy. To the extent permitted by applicable law, Supplier shall take all reasonable actions to prevent disclosure of Unisys Data to law enforcement or any government agencies and/or in response to a legal demand such as subpoena or similar demand, without Unisys's prior express written consent.

2.11 [Client terms flow-down, if any]

3. <u>Subprocessor</u>

4.1 If Supplier uses a Subprocessor to fulfill its obligations under this DPA, it will:

a) Conduct reasonable due diligence to ensure that the Subprocessor can meet the obligations set out herein and in particular provides sufficient guarantees to implement technical and organizational measures in such a manner that the processing will meet the requirements of the applicable data protection laws;

b) Obtain prior written specific or general written authorization from Unisys; In the case of general written authorization, Supplier shall inform Unisys of any intended changes concerning the addition or replacement of other processors, thereby giving Unisys the opportunity to object to such changes.

c) Execute a written contract detailing the terms of the sub-processing activities and provide a copy to Unisys;

d) Ensure that no personal data are transferred outside the EU/EEA, except with prior authorization from Unisys and under a Valid Transfer mechanism; and

e) Ensure any sub-processor adheres to the terms of this DPA as if it were a party to it.

4.2 Supplier shall be liable for the acts and omissions of any Subprocessor to the same extent as if the acts or omissions were performed by Supplier.

5. Supplier Personnel

5.1 Supplier shall take reasonable steps to require screening of its personnel who may have access to Personal Data and shall require such personnel (i) to receive appropriate training on their responsibilities regarding the handling and safeguarding of Personal Data and (ii) to agree to comply with confidentiality obligations which shall survive the termination of employment.

5.2 Supplier will ensure that access to Personal Data is strictly limited to employees who have complied with clause 5.1 above and who need access to Personal data for the agreed Processing.

5.3 If disclosure of Unisys Data is required by applicable law or a compulsory legal process, Supplier shall, unless prohibited by applicable law: (i) notify Unisys promptly in writing before complying with any such disclosure request in order to provide Unisys an opportunity to intervene, if appropriate; and (ii) disclose the minimum amount of Unisys Data necessary to comply with applicable law or a compulsory legal process.

6. Return or Destruction of Unisys Data

6.1 Upon termination or expiration of the Agreement for any reason, or if any part of the Unisys Data retained by Supplier ceases to be required by Supplier to perform its Processing obligations under the DPA, Supplier shall promptly return and delete all Unisys Data in accordance with the relevant provisions of the Agreement and certify in writing to Unisys that it has destroyed or returned all Unisys Data.

7. Security Measures.

7.1 Supplier warrants and undertakes to have in place and shall implement and maintain appropriate organizational and technical processes and procedures designed to protect against any unauthorized or unlawful access, processing, loss, destruction, theft, damage, use or disclosure of Unisys Data or systems, including, at a minimum, the technical and organizational measures set forth in the Data Security Addendum ("DSA"). Unisys reserves the right to restrict, monitor and/or terminate access to its systems and network at any time.

8. Personal Data Breach and Response

8.1 Supplier shall promptly notify Unisys of a Personal Data Breach without undue delay and no later than 24 hours upon Supplier becoming aware of the Personal Data Breach. Supplier should notify Unisys by telephone to Supplier's primary business contact and via email at **unisysglobalprivacy@unisys.com** if it aware that there is, or reasonably believes that there has been, a Personal Data Breach. Notice must include the following:

a) the nature of the Personal Data Breach,

b) the categories and numbers of Data Subjects concerned, and the categories and numbers of records concerned;

c) the name and contact details of Supplier's DPO or other relevant contact from whom more information may be obtained;

d) the likely consequences of the Security Breach; and

e) the measures taken or proposed to be taken to address the Personal Data Breach.

8.2 Supplier shall (i) cooperate with Unisys in the manner reasonably requested by Unisys and in accordance with law to investigate and resolve the Personal Data Breach, and mitigate any harmful effects (ii) promptly implement any necessary remedial measures to ensure the protection of Unisys Data or Unisys systems; and (iii) properly document responsive actions taken related to any Personal Data breach, including, without limitation, post-incident review of events and actions taken to make changes in business practices to ensure the ongoing protection of Unisys Data.

8.3 Except as required by applicable Data Protection Law, Supplier agrees that: (i) it shall not inform any third party of any Personal Data Breach without first obtaining Unisys' prior written consent, other than to inform a complainant that Unisys shall be/has been informed of the Personal Data Breach; and (ii) Unisys 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 any such notice.

8.4 If the Personal Data Breach was a result of Supplier's or Authorized Persons' negligence or breach of the requirements of this DPA, Supplier shall bear all costs associated with (i) the investigation and resolution of the Security Breach; (ii) notifications to individuals, regulators, or others; and (iii) any other remedial actions required by law, recommended by a governmental body or agreed to by the Parties.

If the Personal Data Breach affected Personal Data of US Data Subjects in addition to the above and where available, Supplier agrees to bear the costs associated with i) the provision of two years of credit monitoring by a reputable provider from the date of notification to the individual; and (ii) establishing a toll-free number and call center for affected individuals to receive information.

9. Cross-Border Transfer of Personal Data

9.1 Supplier shall not Process Unisys Personal Data in a jurisdiction outside of the agreed Processing location as set out in Annex II without the written consent of Unisys. To the extent that Unisys provides written consent to the Processing of Personal Data in a third country or in case the Processing activities involve the transfer of Unisys Personal Data from the EEA or Switzerland to locations outside of the EEA (not being countries or territories formally recognized by the European Commission as providing an adequate level of data protection ("Adequate Countries")), Supplier agrees to comply with a Valid Data Transfer Mechanism and inform Unisys thereof prior to Processing outside the agreed location(s).

9.2 If standard contractual clauses are utilized to validate the cross-border transfer of Personal Data, **[*OPTION 1 (USE ATTACHED ANNEX III):*** Supplier shall enter into the standard contractual clauses set forth in Annex III to this DPA**]** **[*OPTION 2 (REMOVE ANNEX III):*** the parties agree that this DPA incorporates by reference the provisions in the European Commission Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries (2010/87/EU) ("Model Processor Contract"), where each of Unisys and/or Unisys' subsidiaries established in the EEA shall be deemed for the purposes of this DPA to be the "data exporter," Supplier and each Subprocessor that stores, accesses, or otherwise processes such Personal Data shall be deemed for the purposes of this Addendum to be a "data importer," the data processing activities in Appendix 1 to the Model Processor Contract shall be as described in Annex II of this DPA, and the data security measures in Appendix 2 to the Model Processor Contract shall be those identified in the Data Security Addendum between the parties. To the extent so requested by Unisys in its sole discretion, Supplier agrees to promptly execute with Unisys and/or any Unisys Affiliate(s) a separate Model Processor Contract with the terms as identified in this Section 9.3**]**.

9.3 The Supplier further acknowledges and agrees that on the request of a competent supervisory authority, enforcement or other public or regulatory authority, client, court or tribunal, Unisys may make available to them a summary or representative copy of this DPA and relevant provisions in this DPA.

9.4 Supplier shall, upon Unisys' request, promptly execute supplemental data processing agreement(s) with Unisys or any of its affiliated companies or take other appropriate steps to address cross-border transfer and other applicable requirements if Unisys concludes, in its sole judgment, that such steps are necessary to address Data Protection Laws applicable to Unisys.

10. General provisions

10.1 **Affiliates**: Unisys is entering into this DPA also on behalf of its Affiliates. Unisys will coordinate all communication with Supplier on behalf of its Affiliates with regard to this DPA. Unisys represents that it is authorized to issue instructions as well as make and receive any communications or notifications in relation to this DPA on behalf of its Affiliates. Unisys Affiliates may enforce the terms of the DPA directly against Supplier subject to the following provisions: (i) Unisys 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 Supplier on behalf of such Affiliate, except where the Data Protection Laws or other applicable 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 Supplier by Unisys of behalf of such Affiliate in accordance with this Section, any losses suffered by the relevant Affiliate may be deemed to be losses suffered by Unisys. If needed for local legal reasons Supplier agrees to enter into a local DPA with the relevant local Affiliate.

10.2 **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 Processing activities under the DPA have ended.

Unisys Entity	Supplier:
By:_____	By:_____
Date: _____	Date: _____

ANNEX I: Definitions

"Data Protection Laws": shall mean 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, EU Data Protection laws and implementation of EU Data Protection laws into national law.

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

"Data Processor": shall mean the entity or "service provider" which Processes Personal data on behalf of the Data Controller.

"Data Subject": shall mean the person to whom the Personal Data relates.

"EEA": shall mean the European Economic Area.

"EU Data Protection law": shall mean: (i) up to 25 May 2018, the Data Protection Directive 95/46/EC; and (ii) from 25 May 2018 onwards the General Data Protection Regulation (EU) 2016/679 **("GDPR")**

"Unisys Data" shall mean any Unisys non-public or proprietary information and data in any form, including Personal Data and Highly Restricted Data, provided by Unisys and its authorized agents or subcontractors or otherwise Processed by Supplier Personnel in connection with the provision of Services under the Agreement.

"Personal Data" shall mean any data relating to (i) an identified or identifiable natural person; (ii) a household; or (3) an identified or identifiable legal entity, where, in case of (ii) and (iii) such information is protected similarly as personal data or personal information under applicable Data Protection Laws.

"Highly Restricted Data" shall mean Social Security or other government issued identification numbers, medical or health information, account security information, unique biometric identifiers, individual financial account information, credit/debit/gift or other payment card information, account passwords, individual credit and income information, intellectual property, proprietary business models, pricing, customer infrastructure/system information or data flows.

"Process" or "Processed" or "Processing" shall mean any operation or set of operations performed on Personal Data or sets of Personal Data, whether or not by automated means, such as, collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Personal Data Breach" shall mean (i) 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 and/or (ii) any security breach and any incident that compromises the security, integrity, confidentiality or availability of Unisys Data or Unisys systems.

"Services" shall mean the services provided or to be provided under the Agreement.

"Subprocessor": shall mean the Supplier and/or a third party entity engaged by Supplier as a Processor under this DPA and approved by the Controller.

"Valid Data Transfer Mechanism": shall mean a data transfer mechanism permitted by EU Data Protection Laws as a lawful basis for transferring Personal Data to a recipient outside the EEA.

ANNEX II: Description of Processing Activity

Identity of Controller

[*For client data, state "The Client of Unisys is the controller."; for all other personal data, state "Unisys and its affiliated companies are the controller."*]

Subject-matter of the processing

[*Please provide details; this should be a high level, short description of what the processing is about i.e. its subject matter*]

Duration of the processing

[*Please provide details clearly set out the duration of the processing including dates*]]

Nature and purpose of the processing

[*Please provide details; please be as specific as possible, but make sure that you cover all intended purposes*

The nature of the processing means any operation such as collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc. The purpose might include, processing for recruitments services, payroll, marketing etc.]]

The type of personal data and categories of Data Subjects

[*Please provide details*] *examples here include, name, address, social security number, date of birth, telephone number, pay, images, bank account numbers, etc.*]

Location of the processing

[*Please provide details where will the processing take place; any export of data outside EEA; a Data flow map could be attached if Suppliers have that available*]

Plan for return of destructing

[*Please provide details; describe how long the data will be retained for, how it be returned or destroyed*

[ANNEX III- Standard Contractual Clauses (processors)]

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:.....

Address: .....

Tel.: ..... ; fax:..... ; e-mail:.....

Other information needed to identify the organisation

……
(the data **exporter**)

And

Name of the data importing organisation: .....

Address: .....

Tel.:.....; fax: ..... ; e-mail:.....

Other information needed to identify the organisation:

……
(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(b) '*the data exporter'* means the controller who transfers the personal data;

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

---

2 Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely …….

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely ……..

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature……..

(stamp of organisation)

On behalf of the data importer:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature……..

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

……
……
……

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

……
……
……..

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

……
……
……

Categories of data

The personal data transferred concern the following categories of data (please specify):

……
……
……

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

……
……
……

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

……
……
……

DATA EXPORTER DATA IMPORTER

Name:……	Name:……
Authorised Signature ……	Authorised Signature ……

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Supplier shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and to protect the Confidential and Personal Data of Unisys and its clients that Supplier processes for Unisys ("Unisys Data") against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Unisys data transmitted, stored or otherwise processed in accordance with the DSA between the parties, which may be attached hereto.

DATA EXPORTER	DATA IMPORTER
Name:……	Name:……
Authorised Signature ……	Authorised Signature ……

APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

Unisys Corporation might sub-contract processing of personal data received from the data exporter to its other subsidiaries and service providers located outside of the EEA (including India, Australia, Brazil and Colombia), subject to such other companies agreeing to be bound by all obligations of the data importer under the Clauses.

The data exporter hereby confirms consent for the data importer to engage as sub-processor other subsidiaries and service providers on the basis set out in this approach.

DATA EXPORTER	DATA IMPORTER
Name:……	Name:……
Authorised Signature ……	Authorised Signature ……