Data Processing Agreement

INSTRUCTIONS ON HOW TO EXECUTE THIS Data Processing Agreement ("Agreement"):

1. This Agreement consists of two parts: the main body of the Agreement, and Annexes A, B, C and D (which includes Appendices 1 and 2).
2. To complete this Agreement, Client must:
    a. Insert its company name and address in the introductory paragraphs below on Page 2.
    b. Complete and sign the signature box on Page 7.
    c. Complete Annex A on Page 8 by supplying details of the data protection officer and/or Article 27 Representative, if applicable. If neither of these apply, supply your contact information for reaching the individual regarding data privacy matters.
        i. Review and update (if needed) Annex A on Page 8, information describing the subject-matter and purpose of the Personal Data processed, the type of Personal Data, the presence of any "Special Categories" of Personal Data as defined under EU 2016/679, and the Data Subjects of the Personal Data processed.
    d. If Personal Data Processed under this Agreement is located in the European Union or European Economic Area, complete the information as the data exporter and sign where indicated in Annex D on Pages 13, 20, and Appendix 1 Page 22.
        i. Complete the governing law in Clauses 9 and 11 on Pages 19 and 20.
3. Submit the completed and signed Agreement to Symmetry by sending to DataPrivacy@SymmetryCorp.com.
    a. Upon receipt at this email address, Symmetry will review the signed Agreement from the Client. If valid, Symmetry will countersign and provide a copy of the fully executed Agreement to Client accordingly. This Agreement will only be considered legally binding upon authorized signature by both Client and Symmetry.

Data Processing Agreement

This Data Processing Agreement ("**Agreement**") forms part of the Master Service Agreement or other written or electronic agreement between:

(i) _____(CLIENT NAME) ("**Client**"), with its principal place of business at _____(CLIENT ADDRESS); and

(ii) Symmetry, LLC, having its principal place of business at 400 S. Executive Drive, Ste. 200, Brookfield, WI 53005, USA ("**Symmetry**" **or** "**Processor**"),

(each a "**Party**" and collectively the "**Parties**").

WHEREAS the Parties are parties to an executed Master Services Agreement ("MSA") dated _____.

WHEREAS Processor may receive or have access to certain Personal Data (defined below) of Client in the course of providing the services under the Master Services Agreement, and the parties hereby wish to establish terms governing the protection of such Personal Data.

By signing this Agreement, Client enters into this Agreement on behalf of itself and, to the extent required under applicable data protection laws and regulations, in the name and on behalf of its Affiliate(s) as defined in the MSA, if and to the extent Processor processes Personal Data for which Client and/or its Affiliates qualify as the Controller.

NOW THEREFORE, the Parties hereby agree to the following terms regarding the data privacy and protection obligations applicable to Processor's handling of Personal Data on behalf of Client in connection with providing the Processing Services (defined below) to Client as Controller.

1. Definitions

a. "Affiliate" means any present or future company that, directly or indirectly, is controlled by or is under common control with the Client. For the purpose of this definition, "control" means the power to exercise a controlling influence over the management or policies of a legal entity, whether by virtue or equity ownership, operating or shareholders' agreement, management agreement, or otherwise.

b. "Personal Data" means any information relating to an identified or identifiable natural person ("Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, biometric data, an online identifier such as an IP address, persistent cookie or device ID, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person to the extent such data derive from an EU Data Subject.

c. "Controller" or "Data Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

d. General Data Protection Regulation ("GDPR") means REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

e. "Processing" means any operation or set of operations which is performed on personal data or on 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.

f. "Processing Services" means the Processor's authorized processing of Personal Data pursuant to the Master Services Agreement between the Processor and the Controller.

g. "Processor" or "Data Processor" means the entity that processes Personal Data on behalf of the Controller.

h. "Subprocessor" means a service provider or supplier to the Processor that is authorized by the Processor in writing to process Personal Data in accordance with the Controller's direction in the Master Services Agreement. The Subprocessor services are part of the Processor's Processing Services for the Controller.

i. "Subprocessing Services" means the Subprocessor's authorized processing of Personal Data pursuant to the Master Services Agreement between the Processor and the Subprocessor. These are specified in Annex A, which incorporates the Controller's instructions to the Processor into instructions for the Subprocessor.

j. "Model Clauses" means the European Commission Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries under Directive 95/46/EC approved by Commission Decision of February 5, 2010, including Appendices 1 and 2 thereto. To the extent the European Commission subsequently amends the Model Clauses at a date later than Agreement Effective Date, the terms existing therein shall supersede and replace any Model Clauses executed between Controller and Processor.

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

l. Defined terms not otherwise defined herein shall have the same meaning provided in the Regulation (EU) 2016/679 of the European Parliament and of the Council also known as the General Data Protection Regulation or ("GDPR").

2. Processing of Personal Data

a. The Parties agree that Client is and shall remain the Controller of Personal Data for purposes of applicable privacy and data protection laws with rights and obligations under such laws to determine the purposes for which Personal Data is processed, including the means by which it may be transferred to a third country or international organization, and nothing in this Agreement shall restrict or limit in any way Client's rights or obligations as Controller of Personal Data for such purposes. As such, Client is instructing Processor to process Personal Data in accordance with the terms of this Agreement as further detailed below.

b. Processor shall only process Personal Data in accordance with the written instructions of and on behalf of Client as Controller, as necessary to carry out the purposes of the Agreement in accordance with this Agreement or as otherwise authorized by Client in writing. The Processing Services currently approved by Client are set out in Annex A, and any instructions for or changes to such Processing Services must be established in writing.

c. Processor will have no liability for any harm or damages resulting from Processor's compliance with instructions received from Client. Where Processor believes that compliance with Client's instructions could result in a violation of Data Protection Laws or is not in the ordinary course of Processor's obligations, Processor shall promptly notify Client thereof. Client acknowledges that Processor is reliant on Client's representations regarding the extent to which Controller is entitled to process Personal Data.

d. Processor shall, within 48 hours, notify Client in writing of any request, complaint, claim or other communication received by Processor or its Subprocessor(s) regarding Personal Data for which Client is Controller: (i) from an individual who is (or claims to be) the Data Subject of the Personal Data; (ii) from any government official (including any data protection agency, law enforcement agency or other regulatory authority); and/or (iii) from Client's employees or other third-parties, other than those set forth in this Agreement. Unless otherwise required by applicable law, Processor shall obtain Client's express written consent before disclosing or sharing any

Personal Data in response to such requests, and Processor shall respond to such requests only when authorized by Client or compelled by a valid legal mechanism or applicable authority to do so. Notwithstanding anything to the contrary, however, Processor shall, at Client's expense, also cooperate with Client and its affiliates and representatives in responding to inquiries, claims and complaints regarding the processing of Personal Data.

e. Processor warrants that its employees have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and that such persons who have access to Personal Data are bound to process Personal Data in compliance with Client's instructions.

f. Upon request, Processor shall, at Client's expense, assist Client in carrying out a data protection impact assessment or similar activity, through reasonable means, including but not limited to, providing a systemic description of the envisaged processing operations, assistance with an assessment of the risks to the rights and freedoms of the Data Subjects to whom the Personal Data relates, and/or an assessment of the necessity and proportionality of the processing operations in relation to the underlying purpose. Processor shall also, at Client's expense, cooperate and provide reasonable assistance or information needed for Client to engage in consultations with regulatory authorities or otherwise respond to requests for information from such authorities.

3. Technical and Organizational Security Measures

a. Processor shall maintain current documentation reflecting its information security program ("Information Security Program") that includes administrative, technical, and physical safeguards that protect the confidentiality, integrity and availability of Personal Data, protect against reasonably anticipated threats or hazards to the confidentiality, integrity and availability of Personal Data, and protect against unauthorized access, use, disclosure, alteration or destruction of Personal Data. Taking into account industry standards, the costs of implementation, the nature, scope, context and purposes of the processing and risks to the rights and freedoms of Data Subjects, Processor agrees to implement commercially reasonable technical and organizational measures to ensure a level of security for Personal Data appropriate to the risk.

b. In addition to any specific and/or supplemental security safeguards established in the Agreement between the parties, Processor's Information Security Program shall include, but not be limited to, the safeguards set forth in Annex B to this Agreement, which is incorporated herein by this reference. To the extent that any specific or supplemental security safeguards in the Agreement are less stringent than the safeguards set forth in Annex B to this Agreement, the terms of Annex B shall take precedence with respect to Personal Data. Upon Client's reasonable request and at Client's expense, Processor shall permit Client to view, but not take possession of, Processor's written information security policy or equivalent third-party audit report or certification establishing that it has implemented the safeguards set out in the Information Security Program.

4. Security Breach Management and Breach Notification

a. Notwithstanding any provisions in this Agreement to the contrary, in the event that: (i) any Personal Data is disclosed by Processor (including its Subprocessors), in violation of this Agreement or applicable laws pertaining to privacy or data security; or (ii) Processor (and, as of May 25, 2018, or any of its Subprocessors) discovers, is notified of or suspects a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by Processor ("Data Breach"), Processor shall notify Client without undue delay in writing of any such Data Breach, cooperate fully in the investigation of the Data Breach, and take reasonable measures to limit further unauthorized disclosure of or other unauthorized processing of Personal Data in connection with the Data Breach.

b. To the extent that a Data Breach gives rise to a legal requirement to provide: (i) notification to public authorities, individuals or other persons; or (ii) undertake other remedial measures (including, without limitation, notice,

credit monitoring services and the establishment of a call center to respond to inquiries (each of the foregoing a "Remedial Action")), at Client's request, Processor shall, at Client's cost, undertake customary, necessary and legally required Remedial Actions.

5. Subprocessors

a. Client acknowledges and agrees that Processor is permitted to use Subprocessors as described in Annex C to perform the Processing Services; and Processor shall remain at all times responsible for and fully liable to Client for its Subprocessors' performance under this Agreement. In addition to the requirements set out in Section 4 ("Security Breach Management and Breach Notification"), Processor maintains written agreements with each authorized Subprocessor that imposes substantially similar or greater obligations as Processor's obligations as set forth under this Agreement. When Processor anticipates the need for a new or different Subprocessor to perform services under the MSA, Processor shall inform Client of the intended changes so as to give Client the opportunity to object to such changes. Client will have seven (7) days from the date of receipt of the notice to approve or reject the change. If Client does not object in this time period, the Subprocessor will be deemed accepted. If Client rejects the replacement Subprocessor, Processor will have thirty (30) days to address the Client's objection. If after thirty (30) days of good faith efforts on the part of Client and Processor, Client still does not provide consent to the proposed change, Processor may terminate the services relying on the replacement Subprocessor with thirty (30) days written notice to Client or in the alternative, Processor may seek alternate Subprocessors for Client's consideration.

6. Data Subject Rights

a. With effect from May 25, 2018, Processor shall, to the extent legally permitted, promptly notify Client if Processor receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("Data Subject Request"). Taking into account the nature of the Processing, Processor shall assist Client by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Client's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Client, in its use of the Services, does not have the ability to address a Data Subject Request, Processor shall, upon Client request, provide commercially reasonable efforts to assist Client in responding to such Data Subject Request, to the extent Processor is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Client shall be responsible for any costs arising from Processor's provision of such assistance.

7. Audit Rights

a. Beginning May 25, 2018, Processor shall, at no additional cost, keep or cause to be kept full and accurate records relating to all processing of Personal Data on behalf of Client as part of the Processing Services, and Client may, no more than once per year, request, upon ten (10) days written notice to Processor (unless a shorter period is required to meet a legal requirement or request by a government authority), access to Processor's facilities, systems, records and supporting documentation in order to audit, itself or through an independent third-party auditor at Client's expense, Processor's compliance with its obligations under or related to this Agreement and its Information Security Program. Audits shall be subject to all applicable confidentiality obligations agreed to by Client and Processor, and shall be conducted in a manner that minimizes any disruption of Processor's performance of services and other normal operations. In the event that any such audit reveals material gaps or weaknesses in Processor's Information Security Program, Client shall be entitled to suspend transmission of Client Personal Data to Processor and terminate Processor's processing of Personal Data until such issues are resolved. Client may also require Processor to, upon request and at Client's expense, make available to Client any information necessary to demonstrate compliance with the obligations set forth in this Agreement.

8. Transfer Mechanisms for Data Transfers

a. Subject to the terms of this Agreement, Processor utilizes The Standard Contractual Clauses set forth in Annex D to this Agreement as an appropriate safeguard for the online transfer of Personal Data under this Agreement from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations of the foregoing territories, to the extent such transfers are subject to such Data Protection Laws and Regulations.

9. Post-Termination

a. Notwithstanding any other provision of this Agreement to the contrary, when Processor (including any of its Subprocessors) ceases to perform Processing Services for Client upon termination of this Agreement or otherwise, Client agrees that Processor shall, at Client's expense, securely purge, delete and destroy Client's Personal Data, unless legislation imposed upon Processor prevents it from returning or destroying all or part of Personal Data transferred; in such case, Processor must communicate in writing the legal basis preventing it from returning or destroying Client's Personal Data. In the event that Processor is prevented from returning or destroying any Personal Data as a result of a legal obligation, Processor warrants that it shall provide for the confidentiality of Client's Personal Data and shall not actively process Personal Data. Electronic media containing Personal Data shall be disposed of in a manner that renders Personal Data unrecoverable. Upon request, Processor shall provide Client with written confirmation of its compliance with this provision.

10. Privacy Contact

a. Processor shall designate a contact person within its organization authorized to respond to inquiries concerning processing of Personal Data and shall fully cooperate with Client concerning all such inquiries if so requested. Processor's contact for receiving Data Privacy inquiries is DataPrivacy@SymmetryCorp.com.

Acceptance

IN WITNESS WHEREOF, the Parties have executed this Agreement and represent that their respective signatories whose signatures appear below are authorized by all necessary corporate action to execute this Agreement.

This Agreement may be executed in one or more counterparts, each of which will be deemed an original, but all of which taken together will constitute one and the same agreement.

CONTROLLER CLIENT	PROCESSOR SYMMETRY, LLC
By:	**By:**
Name:	**Name:** Andy Breton
Title:	**Title:** Chief Financial Officer
Date:	**Date:**

ANNEX A

Please provide the contact information for your data protection officer (if applicable):

_____

Please provide the contact information for your representative under Article 27 (if applicable):

_____

If neither of the above apply, please provide the contact information for the individual that would handle any privacy matters:

_____

At all times, the Client controls what personal information is provided to the Processor, and Processor relies upon Client to provide complete and accurate information in this Annex.

Processor, in normal operations, will not access or view individual records, and has no visibility beyond ad hoc, limited technical support, into Client's information. Processor is reliant upon Client to provide the information below.

1. The subject-matter of the processing is as follows:

   Processor provides services to Client pursuant to the MSA and any supporting Statement(s) of Work).

2. The duration of the processing will be the duration of the MSA and any supporting Statement(s) of Work.

3. The nature of the processing is as follows:

   Client licenses SAP software to manage resources that support ongoing business operations.

   Client has engaged Processor to provide technical services, which may include installation, maintenance, troubleshooting, repair, backup, recovery, hosting and general servicing for the Client's SAP installation and associated data.

4. The purpose of the processing is as follows:

   Processor provides services to Client pursuant to the MSA and any supporting Statement(s) of Work).

5. The Processor is directed by Client as the Controller to perform the following processing activities as applicable to deliver the services in the MSA and associated Statement(s) of Work:

   - Managed SAP Foundation – Processor may access the systems and data to provide technical support of Client's SAP environments. Examples include system tuning and configuration for performance and availability.
   - Managed SAP Security – Processor may access the systems and data to provide services to manage and maintain Client's SAP security and controls environment.
   - SAP Security Implementation and Redesign – Processor may access the systems and data to provide security consulting support to implement SAP Security in new SAP environments, redesign SAP Security in existing environments, or rollout SAP Security for one or more new Client locations.
   - ControlPanelGRC – Processor may provide a software application that will access the systems and data to provide compliance automation for SAP environments.
   - Managed Network Firewall – Processor may provide technical services to install, configure and maintain firewall(s).
   - SAP Hosting – Processor may access the systems and data to provide virtualized hosting for supported SAP products.

ANNEX A

- Managed Private Cloud – Processor may access the systems and data to install and manage applicable licensing for hypervisor and/or virtualization software.
- Managed Storage Area Network – Processor may access the systems and data to provide a managed SAN storage.
- Managed Data Protection – Processor may access the systems and data to provide offsite data replication and retention.
- Network Engineering – Processor may access the systems and data to provide network engineering activities. Examples include load balancing, high availability, high speed internet connectivity, virtual machine management, antivirus, patching, perimeter monitoring, security event monitoring and alerting, and operating system maintenance activities.
- Disaster Recovery as a Service (DRaaS) – Processor may access the systems and data to provide failover to a virtual environment.
- Other Technical Services – Processor may access the systems and data to provide other technical services. Examples include installations, upgrades, migrations, maintenance, and adhoc support of SAP applications and databases, or operating systems.

In performing the above activities, Processor may access, view, copy, store, and transmit the data.

Processor may also correspond or communicate with Client employees, Client's Subprocessors and/or Processor's Subprocessors as indicated in Annex C. Processing activities may involve accessing or transferring a copy of the data processed to a second data facility, which may be in a different country from the primary processing activities. If the transfer of Client's information involves the transfer of information from the European Economic Area ("EEA") to the United States, Annex D will apply as the safeguard for such transfer.

ANNEX B

To the extent that Client provides to Processor or Processor otherwise accesses Client's Personal Data in connection with this Agreement, Processor shall implement an Information Security Program that includes administrative, technical and physical safeguards to protect the confidentiality, integrity and availability of Personal Data, protect against any reasonably anticipated threats or hazards to the confidentiality, integrity and availability of Personal Data, and protect against unauthorized access, use, disclosure, alteration or destruction of Personal Data. In particular, Processor's Information Security Program shall include, but not be limited to the following safeguards where appropriate or necessary to ensure the protection of Personal Data:

1. Access Controls – policies, procedures and physical and technical controls: (i) to limit physical access to its information systems and the facility or facilities in which they are housed to properly authorized persons; (ii) to ensure that all members of its workforce who require access to Personal Data have appropriately controlled access, and to prevent those workforce members and others who should not have access from obtaining access; (iii) to authenticate and permit access only to authorized individuals and to prevent members of its workforce from providing Personal Data or information relating thereto to unauthorized individuals; and (iv) to encrypt Personal Data where appropriate.

2. Security Awareness and Training – a security awareness and training program for all members of Processor's workforce (including management), which includes training on how to implement and comply with its Information Security Program.

3. Security Breach Procedures – policies and procedures to detect, respond to and otherwise address security breaches, including procedures to monitor systems and to detect actual and attempted attacks on or intrusions into Personal Data or information systems relating thereto, and procedures to identify and respond to suspected or known security incidents, mitigate harmful effects of security incidents, and document security incidents and their outcomes.

4. Contingency Planning – policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages Personal Data or systems that contain Personal Data, including a data backup plan and a disaster recovery plan.

5. Device and Media Controls – policies and procedures that govern the receipt and removal of hardware and electronic media that contain Personal Data into and out of a Processor facility, and the movement of these items within a Processor facility, including policies and procedures to address the final disposition of Personal Data and/or the hardware or electronic media on which it is stored, and procedures for removal of Personal Data from electronic media before the media are made available for re-use.

6. Audit Controls – hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information, including appropriate logs and reports concerning these security requirements and compliance with the requirements.

7. Data Integrity – policies and procedures to ensure the confidentiality, integrity and availability of Personal Data and protect it from disclosure, improper alteration or destruction.

8. Storage and Transmission Security – technical security measures to guard against unauthorized access to Personal Data that is being transmitted over an electronic communications network, including a mechanism to encrypt electronic information whenever appropriate, such as while in transit or in storage on networks or systems to which unauthorized individuals may have access.

9. Secure Disposal – policies and procedures regarding the disposal of Personal Data, and tangible property containing Personal Data, taking into account available technology so that Personal Data cannot be practicably read or reconstructed.

ANNEX B

10. Assigned Security Responsibility – a designated security official is responsible for the development, implementation and maintenance of its Information Security Program. That individual is the Chief Technology Officer (CTO).

11. Testing – regular testing conducted at least annually on key controls, systems and procedures of its Information Security Program to ensure that they are properly implemented and effective in addressing the threats and risks identified. Tests are conducted or reviewed by independent third-parties or staff independent of those that develop or maintain the security programs.

12. Adjust the Program – the Information Security Program will be monitored and adjusted as appropriate in light of any relevant changes in technology or industry security standards, the sensitivity of Personal Data, internal or external threats to Processor or Personal Data, requirements of applicable work orders, and Processor's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to information systems.

ANNEX C

Processing activities are supported by the Subprocessors listed below, and Client hereby permits the following subcontractors as Subprocessors pursuant to Section 5 ("Subprocessors") of this Agreement.

Subprocessor/Vendor	Geographic Location	Service Provided
CRM	US	Provides solutions for customer relationship management.
Cyber Security	US	Provides Splunk consulting, ongoing management, and security services to address complex security monitoring, compliance and reporting requirements.
Cyber Security & Identity Management	US	Global cyber security company that develops, markets and supports a family of privileged identity management and vulnerability management products (for Unix, Linux, Windows, and Mac OS operating systems.)
Data Center	Netherlands	Continental Europe Data Center
Data Center	US	East Coast Data Center
Data Center	US	West Coast Data Center
Data Center	US	Midwest Data Center
Data Center	US	Midwest Data Center
Data Center	US	Provides IT infrastructure, business continuity, and resilience solutions.
Data Center Cabling	US	Provides project planning and management, network build and maintenance, and consulting services.
Data Retention	US	Provides tape archival and paper shredding services.
Electronic Signatures	US	Provides electronic signature technology and digital transaction management services for facilitating electronic exchanges of contracts and signed documents.
ITSM Software	US	IT service management software
Microsoft Office	US	Provider for productivity tools for producing documents, collaboration, communication, etc.
Monitoring Software	US	Provides applications and network performance monitoring.
SAP Services	Bulgaria	SAP Partner, providing implementation and support services, business application integration and SAP education and training.
Web Conferencing	US	Provides on-demand collaboration, web conferencing, and videoconferencing applications and services.

ANNEX D

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: Symmetry, LLC

Address: 400 S. Executive Drive, Ste. 200, Brookfield, WI 53005, USA

Tel.: 888-796-2677 fax: 877-834-7881

e-mail: DataPrivacy@SymmetryCorp.com

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;

(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 sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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.

([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.

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 sub-processor 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 sub- processor 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 sub-processor 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 sub-processing 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 sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub- processor 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:

([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.

(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;

(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 sub-processing, 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 sub-processing, it has previously informed the data exporter and obtained its prior written consent;

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

(j) to send promptly a copy of any sub-processor 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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor 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 sub-processor 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 sub-processor, 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 sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, 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

Sub-processing

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 sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses ([3]). Where the sub-processor 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 sub-processor's obligations under such agreement.

([3]) This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

2. The prior written contract between the data importer and the sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing 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 sub-processing 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 sub-processor 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 sub-processor 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): Andy Breton

Position: Chief Financial Officer

Address: 400 S. Executive Drive, Ste. 200, Brookfield, WI 53005, USA

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):

Please refer to Annex A of this Agreement.

Data importer

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

Please refer to Annex A of this Agreement.

Data subjects

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

Please refer to Annex A of this Agreement.

Categories of data

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

Please refer to Annex A of this Agreement.

Special categories of data (if appropriate)

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

Please refer to Annex A of this Agreement.

Processing operations

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

Please refer to Annex A of this Agreement.

DATA EXPORTER

Name: .....

Authorised Signature .....

DATA IMPORTER

Name: Andy Breton

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):

Please refer to Annex B of this Agreement.