Policy:

Data Processing Addendum (with EU Standard Clauses)

Intelligent Technology

This **Data Processing Addendum** (together with Exhibit 1 and its Appendices, the 'Addendum') is between **SP** and the **Customer** who has entered into a **Master Services Agreement**, for SP to provide hosting and/or related Services. It replaces all previously signed Data Processing Addendum(s) (if any). Where signed electronically, and contained within a digital envelope or PDF, signature hereof binds the signer to all annexures and provisions contained within the same digital envelope or PDF.

Company, individual, CC or Partnership			**('Counterpart)**
Company Registration or ID Number		Vat Number	
Physical Address			
Postal Address			
Tel Number		Fax Number	

For and on behalf of Counterpart (who warrants his or her authority)		**For and on behalf of Service Provider**	
Signature		Signature	
Printed Name		Printed Name	
Designation		Designation	
Place		Place	
Date		Date	

1. Introduction

1.1. This Addendum is to address the Customer's compliance obligations under Applicable Data Protection Law and is applicable only if and to the extent that Applicable Data Protection Law applies to the Processing of any Personal Data by SP for Customer in relation to the Services ('Customer Personal Data'). If the entity signing this Addendum is not the Customer under the Agreement, this Addendum is not valid and is not legally binding. End-users are not a party to this Addendum.

2. How to execute this addendum

2.1. This Addendum has been pre-signed on behalf of SP.

2.2. Customer must complete, sign and return a copy of the Addendum to **legalnotice@globalmicro.co.za.**

2.3. This Addendum shall only be effective on the date that SP provides Customer with an acknowledgement of receipt of the fully signed Addendum; and, upon the effective date, the Master Services Agreement shall be amended to incorporate this supplementary Addendum.

3. Interpretation

3.1. "**Customer**" means the Counterpart to this Addendum and the Master Services Agreement;

3.2. "**Master Services Agreement**" or "**MSA**", means the Master Services Agreement concluded between SP and Customer;

3.3. "**Services**" shall have the meaning ascribed to it in the Master Services Agreement;

3.4. For the purposes of this Addendum, the following definitions apply and shall prevail as to any conflict with definitions under the Master Services Agreement.

3.5. "**Affiliate**" means any legal entity that a party owns, that owns a party, or that is under its common ownership. "**Ownership**" means, for the purposes of this definition, control of more than a fifty percent interest in an entity.

3.6. "**Applicable Data Protection Law"** means (i) prior to 25 May 2018, EU Directive 95/46/EC and (ii) on and after 25 May 2018, the EU General Data Protection Regulation (EU) 2016/679 ('**Regulation**'), in each case together with any transposing, implementing, or supplemental legislation; and "**Personal Data**", "**Process / Processing**", "**Controller**", "**Processor**", and "**Data Subjects**" shall have the meanings given to them in Applicable Data Protection Law.

3.7. "**Applicable SP Entity"** means each and any SP entity that is established outside the EEA, to the extent that the Customer (i) stores Customer Personal Data in a data centre outside the EEA operated / utilized by SP or (ii) receives Services in respect of a Customer Configuration located in the EEA from such SP entity.

3.8. "**Customer Configuration**" means an information technology system which is the subject of the Services or to which the Services relate.

3.9. "**End-users**" means Customer's own customers and Affiliates whose Personal Data is Processed by SP through the provision to, or use by, the Customer of the Services.

3.10. "**EEA**" means the European Economic Area.

3.11. "**Model Clauses**" means the standard contractual clauses (processors) for the transfer of personal data west out in the EU Commission Decision of 5 February 2010 (2010/87/EC); and "**Subprocessor**", "**Data Importer**", and "**Data Exporter**" shall have the meanings given to them in the Model Clauses.

3.12. "**SP**" shall have the meaning Global Micro Solutions (Pty) Ltd and its Affiliates;

3.13. "**Security Incident"** means a breach of SP security leading to (i) accidental or unlawful destruction of Customer Personal Data or (ii) loss, alternation, unauthorised disclosure of, or access to Customer Personal Data;

3.14. "**Transfer Protections"** means, in relation to a transfer of Customer Personal Data outside the EEA (including any such transfer to Applicable SP Entities and/or to sub processors of SP or of Applicable SP Entities), measures to enable the transfer to be made in compliance with Applicable Data Protection Laws, including without limitation where the recipient of such data: (1) receives such data in a country that the European Commission has decided provides adequate protection for Personal Data (including where the recipient has subscribed to the Privacy Shield under the European Commission's Implementing Decision (EU) 2016/1250), (ii) has achieved binding corporate rules authorization in accordance with Applicable Data Protection Law, (iii) has executed standard contractual clauses adopted or approved by the European Commission (including Model Clauses under this Addendum) or (iv) has in place an alternative mechanism that complies with Applicable Data Protection Law for the transfer of Personal Data outside the European Union.

4. Processing of Personal Data and Parties obligations

Each party agrees to comply with the obligations that apply to it under Applicable Data Protection Law.

4.1. **Processing of Customer's Personal Data.**

4.1.1. The parties agree that, in respect of Processing of Customer Personal Data through the provision or use of the Services:

4.1.1.1. Customer may be either of the following (a) a Controller of Customer Personal Data, or (b) a Processor when it Processes Customer Personal Data on behalf of its End-users. Consequently, SP is a Processor where Customer is Controller or Processor, or a sub processor when the Customer is acting as a Processor on behalf of its End-users;

4.1.1.2. The subject matter of the Processing in SP's provision and Customer's use of the Services and the detection, prevention and resolution of security and technical issues as provided for in the applicable Master Services Agreement;

4.1.1.3. The duration of the Processing shall be from the date of this Addendum (or, if later, from the date Customer Personal Data is first Processed through the provision or use of the Services) until the Master Services Agreement expires or terminates in accordance with its terms;

4.1.1.4. The purpose of the Processing is to provide Services to Customer under the Agreement and the detection, prevention and resolution of security and technical issues as provided for in the applicable Master Services Agreement and any purposes compatible therewith;

4.1.1.5. The type of Personal Data Processed is any Personal Data provided or made available to SP by or on behalf of Customer or any End-user through the use or provision of the Services; and

4.1.1.6. The categories of Data Subjects whose Personal Data are provided or made available to SP by or on behalf of Customer or any End-user through the use or provision of the Services, including staff, contractors, partners of Customer or End-users and any End-users who are individuals.

4.2. **SP's Responsibilities**

This section 4.2 shall apply with effect on and from 25 May 2018. Where SP is Processing Customer Personal Data:

4.2.1. SP shall Process Customer Personal Data only on Customer's documented instructions, including with regard to transfers of personal data to a third country, or an international organisation (instructions on which are set out in section 4.2.3 below), unless required to do so by applicable law to which SP is subject in such case; SP shall inform Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. The parties agree that this Addendum, the Master Services Agreement and Customer's configuration and use of the Services together constitute Customer's complete and final documented instructions to SP on the Processing of Customer Personal Data.

4.2.2. SP shall ensure that all SP personnel (including staff, agents and subcontractors) who SP authorises to Process Personal Data are subject to a duty of confidentiality (whether contractual or statutory); and

4.2.3. SP shall maintain and implement technical and organisation measures appropriate (having regard to the state of technological development and cost of implementation) to the risk of, and to seek to protect Customer Personal Data against, any Security Incident. Such measures shall include, as appropriate: (a) the pseudonymisation and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing. At a minimum, such measures shall include those set out in the Master Services Agreement. In relation to the security of Customer Configurations, the Customer agrees that those security practices and security Services otherwise detailed in the Master Services Agreement are appropriate for Customer Personal Data (and satisfies SP's obligations under this sub-section), in conjunction with the Customer's obligations regarding security measures set out in the Master Services Agreement;

4.2.4. SP shall not transfer any Customer Personal Data outside of the European Economic Area unless it has taken steps to ensure Transfer Protections, but subject to such Transfer Protections Customer agrees that Customer Personal Data may be Processed in countries where the Applicable SP Entity or its subprocessor s maintain facilities or personnel as necessary so that SP may fulfill its obligations under the Master Services Agreement;

4.2.5. SP shall respond to any Data Subject request to exercise their rights, or any other Data Subject query, regarding Customer Personal Data by either asking the Data Subject to make their request to Customer or notifying the Customer of the same. SP shall assist the Customer in respect of the rights of Data Subjects as follows (and the Customer agrees that this sub0section 4.2.5 only applies to the extent Customer does not itself hold or otherwise have access to the Customer Personal Data, and to the extent to which it is possible for SP to provide such assistance taking into account the nature of the Processing);

4.2.5.1. Assist the Customer to respond to any request from a Data Subject to exercise any of her or his rights under Applicable Data Protection Law (including rights of access, correction, objection, erasure and data portability, as applicable) by providing technical measures to provide Customer, in a manner and to the extent consistent with the functionality of the Services and SPs role as Processor, with the ability itself to access, correct, erase, restrict or export Customer Personal Data. In respect of Customer Personal Data which the Customer receives, stores, or transmits on or using the Customer Configuration, the parties agree that the sole assistance SP shall provide is to permit the Customer, in a manner and to the extent consistent with the functionality of the Services and SP's role as Processor, with the ability itself to access, correct, erase, restrict or export Customer Personal Data. In respect of other Customer Personal Data, at Customer's reasonable request and expense, SP shall provide reasonable and timely further assistance to Customer to respond to any such Data Subject requests.

4.2.5.2. Provide reasonable and timely assistance to Customer, at Customers reasonable request and expense, to respond to any other correspondence, enquiry or complaint from a Data Subject, regulator or other third party in connection with the processing of Customer Personal Data.

4.2.6. If SP becomes aware of a confirmed Security Incident, inform Customer without undue delay and provide reasonable information (to the extent that such information is known or available to SP) and cooperation to Customer so that Customer can fulfil any data breach reporting obligations it may have under (and in accordance with the timescales required by) Applicable Data Protection Law. SP shall further take such any necessary measures and actions to remedy or mitigate the effects of the Security Incident and shall keep Customer informed of material developments in connection with the Security Incident. In respect of Customer Personal Data which the Customer receives, stores, or transmits on or using the Customer Configuration, the parties agree that:

4.2.6.1. SP's obligations under this sub-section 4.2.6 shall be limited to the extent consistent with the functionality of the Services and SP's role as Processor, the monitoring and security Services purchased by the Customer, and the parties' respective security obligations under the Master Services Agreement;

4.2.6.2. SP shall be under no obligation to notify routing security alerts in respect of the Customer Configuration (including without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing or other unauthorised access to traffic data that does not result in access beyond IP addresses or headers, or similar incidents) save as otherwise specifically set out in the Master Services Agreement;

4.2.6.3. SP's remediation and mitigation obligations shall be limited to Security Incidents arising out of breach by SP of its security obligations set out in the Master Services Agreement; and

4.2.6.4. SP's assistance shall be at the Customer's expense save where the confirmed Security Incident is caused by breach of SP of its security obligations set out in the Master Services Agreement;

4.2.7. The Customer acknowledges that SP has no knowledge of the Customer Personal Data received, stored, or transmitted on or using the Customer Configuration. Accordingly, taking into account the nature of the Processing and the information available to SP, SP shall assist Customer in ensuring compliance with Customer's obligations pursuant data protection impact assessments and prior consultation under Applicable Data Protection Law by providing (at Customer's expense) the audit reports specified in the Master Services Agreement and the security tools included in the Services. If, however, SP believes or becomes aware that its Processing of Customer Personal Data is likely to result in a high risk to the data protection rights and freedoms of Data Subjects, it shall inform Customer and provide reasonable cooperation to Customer (at Customer's expense) in connection with any data protection impact assessment that may be required under Applicable Data Protection Law;

4.2.8. SP shall enable Customer to retrieve and/or delete Customer Personal Data before any termination of the Master Services Agreement. Customer instructs SP, after the end of the provision of the Services, to delete all Customer Personal Data in SP's possession or control, including existing copies thereof, but this requirement shall not apply to the extent SP is required by applicable law to retain all or some of the Customer Personal Data or to Customer Personal Data SP has archived on backup systems, which data SP shall securely isolate and protect from any further processing except to the extent required by such law until such time as the relevant backup is destroyed in accordance with SP's standard backup destructions policies; and

4.2.9. SP shall maintain records required by Applicable Data Protection Law and information to demonstrate its compliance with Applicable Data Protection Law in relation to its Processing of Customer Personal Data; and provide the Customer audit reports as otherwise specified in the Master Services Agreement to demonstrate compliance.

4.3. **Sub-processing**

The following provisions shall apply in relation to sub-processing.

4.3.1. Customer authorises SP to engage any Applicable SP Entity, and any third-party subcontractors and/or Resellers and/or Advisors (including but not limited to, Amazon, Microsoft, Google and Alibaba) as subprocessor s in connection with the provision of the Services to Customer. The parties agree that:

4.3.1.1. SP shall maintain and make available to the Customer an up-to-date list of its subprocessor s, giving the Customer notice of any change in subprocessor s prior to any new subprocessor being authorised to Process any Customer Personal Data by updating the list accordingly;

4.3.1.2. SP shall impose written data protection terms on any subprocessor it appoints that require it to Process any Customer Personal Data only to the extent necessary to provide the services for which it has been engaged by SP (and for no other purpose) and to protect the Customer Personal Data to at least the standard required by this Addendum and Applicable Data Protection Law; and

4.3.1.3. SP shall remain liable for any breach of this Addendum that is caused by an act, error or omission of its subprocessor. Customer may object to SP's appointment or replacement of subprocessor by terminating its use of the affected Services for convenience on giving written notice in the manner of on the terms provided in the Master Services Agreement (save that the period of notice given by Customer shall be 7 days', and notice must be given by Customer within 7 days' of SP's notice of appointment or replacement) as it sole and exclusive remedy, without prejudice to any fees incurred by Customer for those Services before any such notice of termination takes effect; and such notice of termination shall be ineffective if SP notifies Customer that the proposed appointment or replacement shall not be effective to the Customer prior to the expiry of the Customer's notice of termination. For the avoidance of doubt, in the event of termination, the Customer shall still be liable for termination on the terms specified in the Master Services Agreement.

4.3.1.4. Customer agrees to SP and the Applicable SP Entity giving any such subprocessor s access to Customer Configuration so that SP or the Applicable SP Entity can deliver the Services under the Agreement. Customer further agrees that those subprocessor s may be based outside of the state, province, country, or other jurisdiction in which Customer has chosen to store Customer Personal Data, subject to SP taking steps to ensure Transfer Protections if transfers are made to subprocessor s. SP requires that its subprocessor s maintain security and data protection practices that are consistent with the Master Services Agreement.

4.4. **Customer Responsibilities**

4.4.1. Customer undertakes that its instructions to SP as its Processor and its use of the Services for Processing Customer Personal Data will each

4.4.1.1. Comply with privacy laws or regulations applicable to its Processing of Customer Personal Data, including Applicable Data Protection Law; and

4.4.1.2. not cause SP to infringe Applicable Data Protection Law. The Customer will ensure that it has all necessary consents, notices and other requirements in place to enable lawful Processing of the Customer Personal Data by SP for the duration and purposes of the Master Services Agreement.

4.4.2. In respect of data which the Customer receives, stores, or transmits on or using the Customer Configuration:

4.4.2.1. In addition to Customer's obligations stated in the Master Services Agreement, the Customer is responsible for the integrity, security, maintenance and appropriate protection of Customer Personal Data, and ensuring its compliance with any privacy laws and regulations applicable to its own Processing of the Customer Personal Data and its use of the Services, including Applicable Data Protection Law;

4.4.2.2. Customer control how Customer Personal Data is stored, classified, exchanged, or otherwise Processed when using the Services;

4.4.2.3. Customer may select the territory which it stores and Processes Customer Personal Data and may implement and maintain or purchase supplementary services from SP or the Applicable SP Entity, in order to put in place those technical and organizational security measures appropriate to the nature and volume of Customer Personal Data that Customer Processes using the Service.

5. Application of and clarification to Exhibit 1

5.1. The parties agree that the Model Clauses set out in Exhibit 1 apply only if:

5.1.1. Customer Personal Data to which Applicable Data Protection Law applies is transferred to the Applicable SP Entity and its subprocessor s located in a country that is outside of the EEA, and

5.1.2. No Transfer Protections other than the Model Clauses have been provided.

5.2. **Relationship**

5.2.1. The parties acknowledge that for the purposes of the Model Clauses (where applicable under this Addendum), the Applicable SP Entity is acting in the capacity of either:

5.2.1.1. A Data Importer when Customer is established in the EEA, or

5.2.1.2. A Subprocessor of Customer when Customer is located outside the EEA and is acting in its capacity as a Data Importer or Subprocessor in the Model Clauses as applicable.

5.2.2. For the purposes of Processing and the transfer of Customer Personal Data from the EEA to the Applicable SP Entity, the applicable Clauses in Exhibit 1 shall be supplemented with the following sections 5.2.2.1 and 5.2.2.2. Such supplementary language addresses practical and operational issues and does not modify the Model Clauses:

5.2.2.1. **Clause 5(f) and 12(2) of the Model Clauses** – **Audit Rights**. Customer agrees that the audit described in 5(f) and 12(2) shall be carried out in accordance with the following provision: SP or the Applicable SP Entity shall engage qualified third party auditors to perform examinations of tis systems and services in accordance with: the best practice recommendations of ISO 270002, for the purposes of auditing SP's compliance with ISO 27001; SSAE 16 and ISAE 3452 compliance frameworks, and the AT 101 compliance framework (based up select Trust Services Principles); and/or equivalent industry standards (the resulting output of such audit activities referred to as "**Third Party Audit Reports**"). SP's annual Service Organisation Control ('SOC") report(s) or suitable equivalent standard(s) as specified by SP are available to Customer upon Customer's request subject to SP's SOC distribution requirements. Subject to the terms of the Master Services Agreement and upon Customer's request with not less than 30 days' notice, the Applicable SP Entity agrees (at Customer's expense) to permit Customer perform reviews of the security of the Services or evaluate and monitor the Applicable SP Entity's compliance with its security obligations set forth under the Addendum (the "**Customer Audits**"). Customer Audits may be conducted by internal or external auditors or personnel of Customer who have entered into a no-disclosure agreement with SP or Applicable SP Entity (collectively, "**Auditors**"). Such Customer Audits shall be conducted strictly in accordance with SP's security policies and procedures and consistent with industry best practices and shall be limited to the security aspects of these SP operated data centres in which the server(s) on which Customer Personal Data is located which are not covered by Third Party Audit Reports or SOC reports. Customer Audits are limited to viewing those Services that the Customer is using under the Master Services Agreement. Such scope does not include (i) viewing any documentation, data or other information that are related to other customers of SP or the Applicable SP Entity, or (ii) interacting with data centre or power equipment in any way that may interfere with the performance of or could otherwise pose a risk to the Services, as determined by SP or the Applicable SP Entity in its sole discretion. The applicable SP Entity agrees to co-operate in a commercially reasonable manner with the Auditors and provide the Auditors with commercially reasonable assistance as they may reasonably request in connection with Customer Audits provided that the Auditors avoid disrupting the Applicable SP Entity's operations during the Customer Audits. In the event that Customer request a Customer Audit more than once in a twelve (12) month period, any additional Customer Audits will be performed at Customer's sole cost and Customer will reimburse the Applicable SP Entity for its reasonable costs associated with such additional Customer Audits. In addition, if any Customer Audit will have a duration of more than three (3) hours or exceed the agreed upon scope (including a request to audit any control that has already been covered in an independent audit report), Customer agrees to tender to the Applicable SP Entity an amount equal to SP's projected costs associated with the Customer Audit as a conditions precedent to permitting Customer to conduct such Customer Audit.

5.2.2.2. **Clause 5(g) and 11 of the Model Clauses – Sub-processing.** In accordance with Clause 5(h) and Clause 11, Customer acknowledges and agrees that the Applicable SP Entity may engage subprocessor s as provided in section 4.3.

5.3. Where the Model Clauses contain any obligation to notify the Data Exporter, the Applicable SP Entity shall make such notification to Customer. When Customer acts in the capacity as Data Importer, Customer agrees to make any required notifications to the Data Exporter.

6. General Provisions

6.1. **Conflicting Terms**

6.1.1. To the extent that the Model Clauses are applicable, the Model Clauses in Exhibit 1 supersede any conflicting terms in the Master Services Agreement and this Addendum as to the specific subject matter of Exhibit 1. To the extent that any provision of the Addendum conflicts with any provision of any other document(s) comprising the Master Services Agreement, the terms of the Addendum shall, as to the specific subject matter of the Addendum, take precedence over the conflicting term(s) of such other document(s).

6.1.2. **Governing Law**

6.1.2.1. To the extent any claim arises under Model Clauses in relation to the processing by the Applicable SP Entity of personal data that Customer stores or otherwise processes using the Services (including any claims by a Data Subject pursuant to Clause 3 or Model Clauses), the Model Clauses shall be governed by and construed in accordance with Clause 9 of the Model Clauses. The parties agree, save as provided above, nothing in this Addendum shall affect the application of the governing law section of the Master Services Agreement, which applies to all other claims brought under the Master Services Agreement and this Addendum.

6.1.3. **Limitation of Liability**

6.1.3.1. Customer agrees to exercise its remedies, including those of its Affiliates arising out of or related to this Addendum and the Model Clauses solely against SP (and SP accepts liability in respect of each Applicable SP Entity accordingly). Customer's remedies including those of its Affiliates, arising out of or related to this Addendum and the Model Clauses will be subject to those limitations of liability which apply to Customer under the Master Services Agreement and the aggregate liability to Customer of SP and (if applicable) the Applicable SP Entities collectively under the Master Services Agreement, this Addendum and the Model Clauses in relation to the Processing of Customer Personal Data shall not exceed the lesser of (i) the maximum liability of SP to Customer under the Master Agreement or (ii) one million dollars (US$1,000,000). The Applicable SP Entity is not liable for SP's acts or omissions, non-performance or performance of the Master Services Agreement. This Section 6.1.3 shall not vary Clause 6 of Model Clauses. SP and the Applicable SP Entity are not liable for any claim brought by Customer or any third party (including without limitation and Data Subject, or regulatory or supervisory authority) arising from their compliance with Customer's instructions.

6.1.4. **Third party beneficiaries**

6.1.4.1. Notwithstanding anything to the contrary in the Agreement, where the Applicable SP Entity receives a transfer of Customer Personal Data is not a party to the Master Services Agreement, the Applicable SP Entity will be a third party beneficiary of the Master Services Agreement and this Addendum (including without limitation Section 6.1.3).

6.1.4.2. SP and Customer further agree that, with the exception of (a) Exhibit 1 to which the Data Subjects are third-party beneficiaries, and (b) those provisions of the Master Services Agreement that are relevant to the services provided by the Applicable SP Entity and to which the Applicable SP Entity is a beneficiary, the Master Services Agreement does not confer any rights to any End-Users, Data Subjects, or any other third party. This Addendum does not establish any direct rights of Customer's respective End-Users against SP or the Applicable SP Entity regarding the delivery of the Services.

6.1.5. **No further amendment**

6.1.5.1. All terms and conditions in the Master Services Agreement save as amended herein remain in full force and effect and are binding up the parties.

6.1.6. **Modification**

6.1.6.1. SP may amend or supplement this Addendum, after giving prior notice to the Customer if and to the extent necessary to comply with applicable law or requirement of any supervisory, regulatory or government authority; to implement any standard contractual clauses adopted by the European Commission or a supervisory authority under the Regulation; to comply with any certification grant to SP under the Regulation; or to adhere to a code of conduct approve under the Regulation.

7. Term and termination

7.1. This Addendum and the Model Clauses will terminate contemporaneously and automatically with the termination or expiration of the Agreement.

7.2. SP may terminate the Model Clauses (where applicable under section 3) if SP offers alternative mechanisms to Customer that comply with Applicable Data Protection Law regarding the transfer of Customer Personal Data outside the EEA.

Policy:

Exhibit 1 – Standard Contractual Clauses (processors)

Intelligent Technology

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 the Customer that is a party to the Addendum to which these Standard Contractual Clauses are attached AND the Applicable SP Entity, as described in the Addendum to which these Standard Clauses are attached, 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; [If these Clauses are governed by a law which extends the protection of data protection laws to corporate persons, the words "except that, if these Clauses govern a transfer of data relating to identified or identifiable corporate (as well as natural) persons, the definition of "personal data" is expanded to include those data" are added.]

(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; [If these Clauses are not governed by the law of a Member State, the words "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" are deleted.]

(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; [If these Clauses are not governed by the law of a Member State, the words "within the meaning of Directive 95/46/EC" are deleted.]

(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

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;

(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.

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.

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.

Policy:

Appendix 1 to the Standard Contractual Clauses

Intelligent Technology

This Appendix forms part of the Clauses

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

Terms used in this Appendix 1 have the meaning given to them in the Data Processing Addendum to which these Standard Contractual Clauses have been appended

"Data Exporter" means the Customer or its End-users located in the EEA
"Data Importer" means the Applicable SP Entity where Customer transfers to SP any Customer Personal Data to which Applicable Data Protection Law applies.

The **Data Subjects**, **Categories of Data** and **Processing Operations** are set out in section 4.1 of the Addendum.

Policy:

Appendix 2 to the Standard Contractual Clauses

Intelligent Technology

This Appendix forms part of the Clauses

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

The Applicable SP Entity shall implement security measures at least equivalent to those described in the underlying Master Services Agreement between SP and Customer.