DATA PROCESSING AGREEMENT – FOR SUPPLIERS

MCI XXX, address,

(hereinafter "**MCI**", the "**Data Controller**" or the "**Data Exporter**")

and

[...],

(hereinafter the "**Data Processor**" or the "**Data Importer**")

(both collectively referred to as the "**Parties**" or individually a "**Party**".)

This agreement contains:

- **ANNEX 1 Description of the technical and organizational security measures**
- **ANNEX 2 Standard Contractual Clauses**
- Appendix 1 to the Standard Contractual Clauses
- Appendix 2 to the Standard Contractual Clauses.

I. Subject of the Agreement

The purpose of these clauses is to define the conditions under which **the processor [XXX] ("Processor" or "Service Provider")** undertakes to carry out the personal data processing operations defined below on behalf of **MCI, the data controller**.

As part of their contractual relationship, the parties undertake to comply with the regulations in effect applicable to personal data processing and in particular, Regulation (EU) 2016/679 applicable from 25 May 2018 (hereinafter the "General Data Protection Regulation" or "GDPR").

Under the terms of this rider, the following terms are defined as follows:

- "data controller": the natural person or legal entity, public authority, service or other organisation which, solely or jointly with others, determines the purposes and methods of processing; where said processes and methods are determined by European Union law or the law of a Member State, the controller may be appointed or the specific criteria applicable to their appointment may be provided for by European Union law or the law of a Member State.
- "processor": the natural person or legal entity, department or other organisation that processes personal data on behalf of the data controller.

II. Description of the processing carried out by processors

The processor is authorised to process personal data on behalf of the data controller that are necessary to provide the following service(s) [...].

The details of the processing carried out by processors are as follows:

Nature of the operations carried out on the data (e.g. data storage)	
Purpose(s) of processing	
Categories of personal data processed	
Categories of persons concerned	
Period of data retention or criterion justifying the retention of data (separate from the term of the contract)	
Processor contact person	

This rider is valid as a written instruction for the processing of data by the processor.

III. Processor's obligations in respect of the data controller

The processor undertakes to:

1. process the data solely for the purpose(s) of the subcontracting

2. **process the data in accordance with the data controller's documented instructions.** If the processor considers that an instruction constitutes an infringement of the General Data Protection Regulation or any other provision of European Union law or the law of Member States on data protection, it must inform the data controller immediately.

3. **unless otherwise specifically and expressly authorised by the data controller, process data exclusively within the territory of an EEA Member State.** The processor undertakes not to disclose, make accessible or transfer any of the data controller's data, even for routing purposes, to any processing organisation or processor based in a country located outside the EEA, except with the data controller's prior written consent.
The data controller reserves the right to carry out any checks it deems necessary to confirm the performance of the obligations arising under this clause.

In the event of a transfer outside the EEA, authorised by the data controller, said transfer may only take place within the strict limits necessary for the performance of the services, and provided said transfer is towards a State whose legislation in respect of personal data protection has been recognised by the European Commission as offering an equivalent level of protection, or is governed by standard contractual clauses issued by the European Commission or is carried out on the basis of any other alternative arrangements recognised by the General Data Protection Regulation, subject to data controller's prior agreement to said arrangements in writing. The subcontractor undertakes to append to the present contract the documentary evidence allowing him to make such a transfer.
The processor will ensure that its own processors sign and comply with the requirements of this clause.

4. **guarantee the confidentiality of the personal data processed under this contract**

5. **ensure that those authorised to treat personal data according to this contract:**
   - undertake to respect confidentiality or are subject to an appropriate statutory confidentiality obligation
   - receive the necessary training in respect of personal data protection

6. **take account of data protection principles and data protection by default from the design stage onwards of tools, products, applications and services**

IV. Subcontracting

The processor may call on another processor (hereinafter "the subsequent processor") to carry out specific processing activities. In this case, they must inform the data controller in advance, and in writing, of any planned

changes with regard to adding or replacing other processors. This information must clearly indicate the processing activities subcontracted, identity and contact details of the processor and dates of the subcontracting agreement. The data controller has a minimum period of one (1) month from the date of receipt of said information to present its objections. Said subcontracting may only proceed if the data controller has not expressed an objection during the agreed period.

The subsequent processor is obliged to fulfil the obligations set out in this contract on behalf of the data controller and in accordance with their instructions. It is the initial processor's responsibility to ensure that the subsequent processor offers the same sufficient guarantees in respect of the implementation of appropriate technical and organisational measures to ensure that the processing meets the requirements of the General Data Protection Regulation. Should the subsequent processor fail to fulfil their obligations in respect of data protection, the initial processor shall retain full responsibility in respect of the data controller for the other processor's fulfilment of its obligations.

V. Data subjects' right to information

In the event that the data controller authorises the processor to this effect, it will be the latter's responsibility to provide information relating to the data processing carried out by it to the data subjects concerned by the processing operations at the time the data are collected. The formulation and format of the information must be agreed with the data controller before the data are collected.

VI. Exercise of individual rights

So far as possible, the processor must help the data controller to fulfil its obligation to respond to requests to exercise their rights by data subjects, including rights of access, correction, deletion and opposition, right to restriction of processing, right to data portability and right not to be the subject to an automated individual decision (including profiling).

Should the persons concerned make a request to exercise their rights to the processor, said processor must send such requests, on receipt, by e-mail to anne.lesca@mci-group.com, MCI Data Protection Officer.

VII. Notification of breaches of personal data

The processor must notify the data controller of any personal data breach within a maximum of 24 hours after becoming aware of it, by e-mail to the data protection officer. Said notification must be accompanied by any documentation that may be useful in enabling the data controller to inform the relevant regulatory authority of the breach, if applicable.

The processor must, throughout the period of the Contract, set up and maintain a process and procedures to manage security incidents (including, in particular, breaches of personal data) and ensure continuity of service in accordance with industry standards. The processor (i) shall notify the data controller of the name and contact details of one of its employees, who shall act as the data controller's primary point of contact in respect of security issues and be available 24/7 to deal with any security incidents. Any request from the data controller relating to security must be treated diligently and as a priority by the processor.

Without prejudice to the data controller's other rights and remedies, in the event of a presumed or proven security incident or breach of personal data, the processor must advise the data controller immediately and at the latest, within 24 hours following the occurrence of the security incident or breach of personal data.
Immediately after said notification, the Parties will coordinate their actions in order to investigate the security incident concerned. The processor undertakes to cooperate fully with the data controller, at its own expense, to help it to manage the situation, including but not limited to: (i) helping it with any investigation; (ii) providing the data controller or an independent third party appointed by the data controller with physical access to the facilities and operations concerned; (iii) organising interviews with the employees of the data controller and all other appropriate individuals; and (iv) providing all registers, logs, files, data communications and other relevant documents necessary for compliance with laws, regulations and industry standards or as required by the data controller.

The processor will also provide all reasonable assistance to the data controller in the case of a notification in respect of any action the latter may be obliged or may choose to take in respect of a personal data breach. The processor undertakes not to inform third parties, including the persons concerned, of any breach of personal data without having obtained the prior consent of the data controller in writing, except in the cases provided for in the General Data Protection Regulation. Moreover, the processor acknowledges that the data controller has sole authority to determine: (i) whether or not the breach of personal data must be notified to any individual, regulatory authority, administrative authority or other person pursuant to the General Data Protection Regulation; and (ii) the content of said notification. Where the General Data Protection Regulation requires that

the data controller notify the breach of personal data to the persons concerned, it is understood that the processor will bear all the costs associated with said notification.

The processor shall take the appropriate measures, at its own expense, to mitigate the consequences of any security incident and remedy it, and shall make all the amendments it judges necessary in order to avoid any reoccurrence of an incident of this kind. The processor shall assist the data controller, at its own expense, with restoring the data controller's data in the event of a data loss caused by any failure to fulfil its regulations in respect of the Contract.
The processor shall cooperate and provide the data controller with the necessary assistance in respect of any complaint formulated by a data subject or any investigation or request issued by a regulatory authority with regard to the General Data Protection Regulation or any other applicable regulation.

The processor will reimburse the data controller for the actual costs the latter incurs in providing a response to any security incident and mitigating the harm caused as a result of said incident including, among other things, the cost of investigations, notifications and/or corrective measures. Where the General Data Protection Regulation requires the data controller to notify a breach of personal data, the processor will cover the costs associated with said notification.

It is expressly agreed between the Parties that in the event of a breach of personal data, the following harm shall be deemed direct: (i) reasonable and necessary expenses for investigation and remediation; (ii) reasonable and necessary costs of notification, where such a notification is required by the applicable regulations and (iii) penalties, damages, amounts paid in respect of settlements, reimbursements, compensation and other costs related to the fulfilment of obligations arising from a judgment, settlement or the applicable regulations (the "Losses"), insofar as said losses are due to a failure by the processor to fulfil its contractual obligations.

The processor shall maintain a record of security incidents and make this available to the data controller, including but not limited to breaches of personal data, and shall document all relevant information concerning the circumstances of said incidents and breaches, the harm caused and corrective measures taken to mitigate their effects, as well as the actions and measures taken to avoid any repetition of such incidents or breaches.

VIII. Assistance from the processor in relation to the data controller's fulfilment of its obligations

The processor shall cooperate with the data controller and use its best endeavours to help the data controller prove that it is compliant with all its legislative and regulatory obligations, notably in respect of the General Data Protection Regulation.

In particular, the processor shall, where relevant, assist the data controller with carrying out impact analyses in respect of data protection.

The processor shall, where relevant, also assist the data controller in carrying out a prior consultation with the regulatory authority.

IX. Security measures

The processor acknowledges that security is a fundamental criterion for the data controller and that the processor's compliance with the security requirements defined in the annex 1 to this contract is an essential and decisive obligation for the data controller's consent thereto.

The Processor undertakes to detail in annex to this contract the security measures taken to ensure the security of the processing of personal data carried out on behalf of the data controller, in accordance with article 32 of the GDPR.

X. Retention of data

Once the provision of services relating to the processing of these data is complete, the processor undertakes to:

- Destroy all personal data or
- At any time, at the data controller's written request and at the latest, within 15 calendar days of the end of the Contract, the processor undertakes to return the data controller's personal data, in a legible or interoperable form agreed between the Parties and to destroy all copies (paper or electronic) of the data controller's personal data that it may hold.

The return of all files, data, programmes, documentation, etc. is included in the price for the provision of the Service.

The processor must confirm the actual destruction of the data controller's personal data within 15 calendar days of the data controller's request or the end of the Contract.

The data controller reserves the right to carry out any checks it deems necessary to confirm the performance of these obligations.

This clause will remain in effect after the expiry or termination of the Contract for any reason whatsoever.

XI. Register of categories of processing activities

The processor declares that it holds a written record of all categories of processing activities carried out on behalf of the data controller including:

- the name and contact details of the data controller on behalf of whom it is acting, any processors and, if applicable, the data protection officer;
- the categories of processing activities carried out on behalf of the data controller:
- if applicable, any transfers of personal data to a third country or international organisation, including the identification of said third country or international organisation and, in the case of transfers referred to in clause 49, paragraph 1, second subparagraph of the General Data Protection Regulation, documents attesting to the existence of appropriate guarantees;
- as far as possible, a general description of technical and organisational security measures, including but not limited, as required, to:
    - pseudonymisation and encryption of personal data;
    - means of guaranteeing the constant confidentiality, integrity, availability and resilience of processing systems and services;
    - means of re-establishing the availability of personal data and access thereto in an appropriate time frame in the event of a physical or technical incident;
    - a procedure for regularly testing, analysing and evaluating the effectiveness of technical and organisational measures to ensure the security of processing.

XII. Documentation

The processor shall provide the data controller with the necessary documentation to demonstrate compliance with all its obligations and to enable audits and inspections to be carried out by the data controller or another auditor appointed by it, and to contribute to said audits.

XIII. Audit

Throughout the term of the Contract, the data controller may carry out tests and audits of all or some of the services, either itself or through an independent third party at its expense – subject to five (5) working days' notice – including at the premises of authorised processors, in order to ensure compliance with the stipulations of the Contract in terms of:

- compliance with Security Policies,
- quality of service,
- maintenance of appropriate security measures, in particular to ensure the integrity and confidentiality of the Data Controller's data.

Where the services involve the processing of personal data, the audit may also relate to the verification of the General Data Protection Regulation and the verification of:

- locations used for the processing and/or storage of personal data;
- transfers of personal data outside the European Economic Area;
- measures taken to ensure the security of personal data and combat breaches of personal data.

The processor undertakes to authorise the data controller, or the companies appointed by the latter and tasked with carrying out the audit, to access the necessary information to carry out their mission properly and access the sites where the services are delivered.
The processor will cooperate fully (and, where processors and representatives are concerned, ensure their cooperation) with the data controller and, depending on the case, the audit representatives of the data controller, including giving them access to the premises, personnel, physical and technical environments, equipment, software, documentation, data, registers and systems relating to the services, and any useful information that might reasonably be necessary in carrying out the audit.
An audit report must be sent to the processor.
The processor also authorises the data controller to carry out or arrange for security tests to be carried out continuously to check that the processor's systems are not vulnerable (for example, because of a defective configuration or update) and detect any change likely to expose data to the risks of intrusion.
Moreover, the data controller may carry out any investigations on the internet to detect proven breaches of personal data.

Should it become apparent, following the audit and testing measures described above, that the security measures implemented by the processor are not appropriate or sufficient, or if said audits or tests reveal any gaps or examples of non-compliance with the requirements set out in this Contract and/or the legal

requirements applicable and/or the standards in effect, the processor will implement corrective actions within a time frame to be agreed between the Parties, depending on the severity of the failure observed and in any case, not longer than 15 days, without prejudice to the data controller's additional rights to seek damages and/or terminate the Contract. Audit costs will be payable by the processor in the event of any failings identified in the audit.

XIV. Data controller's obligations in respect of the processor

The data controller undertakes, throughout the term of the contract, to:

1. provide the processor with the data referred to in clause II;
2. document in writing any additional instructions regarding the processing of data by the processor;
3. ensure, prior to and during the period of processing, compliance with the obligations set out in the General Data Protection Regulation by the processor;
4. supervise the processing, including carrying out audits and inspections at the processor's premises in accordance with the provisions of this rider.

Data controller – MCI	Data processor
Date Name Signature	Date Name Signature

Annex 1 – Technical and organisational measures

In addition to any measures already agreed to by the Data Processor, the Data Processor undertakes to institute and maintain the following data protection measures:

1. Access control to Personal Data

The Data Processor commits that the persons entitled to use any data processing system in relation to the Personal Data are only able to access the Personal Data within the scope and to the extent covered by the respective access permission (authorization).

This shall in particular be accomplished by:

- Establishing access authorizations for employees and third parties, including the respective documentations;
- Code card passes;
- Restrictions on keys;
- All required internal regulations;
- Identification of the persons having access authority;
- Securing any and all data processing equipment and personal computers.
- Locking of terminals;
- Allocation of individual terminals and/or terminal user and identification characteristics exclusive to specific functions;
- Functional and/or time restricted use of terminals and/or terminal users and identification characteristics;
- Regulations for user authorization;
- Obligation to comply with data secrecy;
- User codes;
- Differentiated access regulations (e. g. partial blocking);
- Regulations for the organisation of files;
- Logging and analysis of use of the files;
- Controlled destruction of Personal Data, when relevant;
- Work instructions for templates for the registration of Personal Data;
- Checking, adjustment and controlling systems.

2. Transmission control

The Data Processor shall be obliged to enable the verification and tracing of the locations/destinations to which the data subject's Personal Data are transferred by the utilization of the Data Processor's data communication equipment/devices.

This shall be accomplished by: [List all the measures]

3. **Organisation control**

The Data Processor shall maintain its internal organisation in a manner that meets the requirements of this Agreement.

This shall be accomplished by:

- Internal data processing policies and procedures, guidelines, work instructions, process descriptions and regulations for programming, testing and release, insofar as they relate to the Personal Data transferred by the Data Controller;
- Formulation of a data security concept;
- Industry standard system and program examination;
- Formulation of an emergency plan (backup contingency plan).
- Binding policies and procedures for the Data Processor's employees;
- [...]

Annex 2 – EU standard contractual clauses

Name of the data exporting organisation:

MCI XXX, address

(hereinafter the "**Data Exporter**")

and

[...],

(hereinafter the "**Data Importer**")

(both collectively referred to as the "Parties" or individually a "Party".)

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.

It is specified and accepted by Parties that any reference to the 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 shall be interpreted as to a reference to 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 (General Data Protection Regulation - GDPR).

Should a processing of personal data be subject to Swiss law, in particular due to the establishment of the data exporter in Switzerland, any reference to the Directive 95/46/EC shall be deemed to be a reference to the Swiss Federal Act on Data Protection (FADP) as well as its applicable ordinances. Therefore, definitions given to the terms « personal data » and « data subject » shall, in any case, have the meaning given to them in the FADP. The « special categories of data » shall have the meaning of « sensitive data » according to the FADP.

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 or when the data exporter is established in Switzerland the same meaning as in the Swiss Data Protection Act;

(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 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 the GDPR;

(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. When the data exporter is established in Switzerland, any reference to the Directive 95/46/EC of 24 October 1995 shall be interpreted as a reference to the Swiss Data Protection Act and any reference to the Member State in which the data exporter is established as Switzerland.

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.

MCI	_____ (Data Processor)
Signature_____	Signature_____
Name	Name
Title	Title
Date Signed	Date Signed

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 MCI XXX, address

Data importer

The Data Importer is [...].
The Data Importer will be provided with the Personal Data in order to [describe the purpose of the data transfer]

Data subjects

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

Categories of data

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

- [...]

[.....
.....]

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify if there are any):
[.....
.....]

Processing operations

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

DATA EXPORTER

Name:.....

Authorized Signature .....

DATA IMPORTER

Name:.....

Authorized Signature .....

Appendix 2 to the Standard Contractual Clauses

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

The technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) are described in Annex 1 of this Data Processing Agreement and which is included by reference