DATA PROCESSING AGREEMENT

Module 3 - Data Processor to Sub-contractor

Please use this DPA for contracts with operational third-parties acting on behalf of mci group for a client's project. (This DPA is not applicable for contracts with back-office suppliers such as payroll, IT support, consulting, office security suppliers.... For these suppliers please refer to the DPA module 2.)

between

Please specify the mci group entity name XXX, address,
(hereinafter the "**Data Processor**" acting on behalf of its client, the "Data controller")

and

[...],

(hereinafter the "**Sub-Processor**")

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

I. Subject of the Agreement

The purpose of these clauses is to define the conditions under which **the Sub-Processor** undertakes to carry out the personal data processing operations defined below on behalf of **the Data Processor** .

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 as per the Art.4 of the EU GDPR:

- "personal data" means any Information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person Is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- "controller" means the natural legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes

and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

- "processor" means or legal natural person, public authority, agency or other body which processes personal data on behalf of the controller.
- "sub-processor": the natural person or legal entity contracted by the Data Processor to process personal data for the purpose of carrying out a specific processing activity on behalf of the Data Controller.

II. Description of the processing carried out by the sub-processor

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

The details of the processing carried out by sub-processor are specified in Annex I.A.

III. Sub-processor's obligations in respect of the data processor

The sub-processor undertakes to:

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

2. process the data in accordance with the data processor's documented instructions. If the sub-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 processor immediately.

3. unless otherwise specifically and expressly authorised by the data processor, process data exclusively within the territory of an EEA Member State. The sub-processor undertakes not to disclose, make accessible or transfer any of the data processor's data, even for routing purposes, to any processing organisation or processor based in a country located outside the EEA, except with the data processor's prior written consent.
The data processor 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 processor, 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 (please refer to the Annex II) or is carried out on the basis of any other alternative arrangements recognised by the General Data Protection Regulation, subject to data processor's prior agreement to said arrangements in writing. The sub-processor undertakes to append to the present contract the documentary evidence allowing him to make such a transfer.
The sub-processor will ensure that its own data 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 sub-processor has the data processor's general authorisation for the engagement of subcontractors from an agreed list (please refer to the Annex I.C). The sub-processor shall specifically inform in writing the data processor of any intended changes of that list through the addition or replacement of subcontractors at least one month in advance, thereby giving the data processor sufficient time to be able to object to such changes prior to the engagement of the concerned subcontractor(s). The sub-processor shall provide the data processor with the information necessary to enable the data processor to exercise the right to object.

Where the sub-processor engages a subcontractor for carrying out specific processing activities (on behalf of the data processor), it shall do so by way of a contract which imposes on the subcontractor, in substance, the same data protection obligations as the ones imposed on the sub-processor in accordance with these Clauses. The sub-processor shall ensure that the subcontractor complies with the obligations to which the sub-processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

At the data processor's request, the sub-processor shall provide a copy of such a subcontractor agreement and any subsequent amendments to the data processor. To the extent necessary to protect business secret or other confidential information, including personal data, the sub-processor may redact the text of the agreement prior to sharing the copy.
The sub-processor shall remain fully responsible to the data processor for the performance of the subcontractor's obligations in accordance with its contract with the sub-processor. The sub-processor shall notify the data processor of any failure by the subcontractor to fulfil its contractual obligations.

The sub-processor shall agree a third party beneficiary clause with the subcontractor whereby - in the event the sub-processor has factually disappeared, ceased to exist in law or has become insolvent – the data processor shall have the right to terminate the subcontractor contract and to instruct the subcontractor to erase or return the personal data.

V. Data subjects' right to information

In the event that the data processor authorises the sub-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 processor before the data are collected.

VI. Exercise of individual rights

So far as possible, the sub-processor must help the data processor 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 sub-processor, said sub-processor must send such requests, on receipt, by e-mail to privacy@mci-group.com, mci group Data Protection Officer.

VII. Notification of breaches of personal data

The sub-processor must notify the data processor 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 processor to inform the relevant regulatory authority of the breach, if applicable.

The sub-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 sub-processor (i) shall notify the data processor of the name and contact details of one of its employees, who shall act as the data processor'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 processor relating to security must be treated diligently and as a priority by the sub-processor.

Without prejudice to the data processor's other rights and remedies, in the event of a presumed or proven security incident or breach of personal data, the sub-processor must advise the data processor 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 sub-processor undertakes to cooperate fully with the data processor, 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 processor or an independent third party appointed by the data processor with physical access to the facilities and operations concerned; (iii) organising interviews with the employees of the data processor 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 processor.

The sub-processor will also provide all reasonable assistance to the data processor 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 sub-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 processor in writing, except in the cases provided for in the General Data Protection Regulation. Moreover, the sub-processor acknowledges that the data processor 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 processor notify the breach of personal data to the persons concerned, it is understood that the sub-processor will bear all the costs associated with said notification.

The sub-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 sub-processor shall assist the data processor, at its own expense, with restoring the data processor's data in the event of a data loss caused by any failure to fulfil its regulations in respect of the Contract.
The sub-processor shall cooperate and provide the data processor 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 sub-processor will reimburse the data processor 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 processor to notify a breach of personal data, the sub-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 sub-processor to fulfil its contractual obligations.

The sub-processor shall maintain a record of security incidents and make this available to the data processor, 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 sub-processor in relation to the data processor's fulfilment of its obligations

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

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

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

IX. Security measures

The sub-processor acknowledges that security is a fundamental criterion for the data processor and that the sub-processor's compliance with the security requirements defined in the Annex I.B to this contract is an essential and decisive obligation for the data processor's consent thereto.

The sub-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 processor, in accordance with article 32 of the GDPR. The details of the security measures are specified in Annex I.B.

X. Retention of data

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

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

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

- the name and contact details of the data processor 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 processor:
- 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 sub-processor shall provide the data processor with the necessary documentation to demonstrate compliance with all its obligations and to enable audits and inspections to be carried out by the data processor or another auditor appointed by it, and to contribute to said audits.

XIII. Audit

Throughout the term of the Contract, the data processor 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 processor'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 sub-processor undertakes to authorise the data processor, 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 sub-processor will cooperate fully (and, where processors and representatives are concerned, ensure their cooperation) with the data processor and, depending on the case, the audit representatives of the data processor, 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 sub-processor.
The sub-processor also authorises the data processor to carry out or arrange for security tests to be carried out continuously to check that the subprocessor'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 processor 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 sub-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 sub-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 processor's additional rights to seek damages and/or terminate the Contract. Audit costs will be payable by the sub-processor in the event of any failings identified in the audit.

XIV. Data processor's obligations in respect of the sub-processor

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

1. provide the sub-processor with the data referred to in clause II;
2. document in writing any additional instructions regarding the processing of data by the sub-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 sub-processor;
4. supervise the processing, including carrying out audits and inspections at the sub-processor's premises in accordance with the provisions of this rider.

Data processor – Please specify the mci group entity name	Sub-processor - XXX
Date Name Signature	Date Name Signature

ANNEX I

ANNEX I.A

Description of Processing

Categories of data subjects whose personal data is processed

.....

Categories of personal data processed

.....

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

..... Purpose of processing

.....

Nature of the operations carried out on the data (e.g. data storage).....

Period of data retention or criterion justifying the retention of data (separate from the term of the contract).....

Processor 's DPO contact details

.....

.....

For transfers to subcontractors, also specify subject matter, nature and duration of the processing

.....

Supervisory Authority

Identify the competent supervisory authority/ies in accordance with Clause 12 of Annex II

Autorité de protection des données (APD) - Belgium.....

ANNEX I.B

TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

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

Access control to Personal Data

The sub-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.

Transmission control

The sub-processorshall 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 sub-processor's data communication equipment/devices.

This shall be accomplished by: [Sub-processor has to list all the measures]

Organisation control

The sub-processorshall 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 Processorr;
- 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 sub-processor's employees;
- To be completed by the sub-processor [...]

ANNEX I.C

List of subcontractors

The data processor has authorised the use of the following sub-contractors:

Sub-contractors located in the EEA or in an adequate third-country	Sub-contractors not located in the EEA nor in an adequate third-country
Name: … Address: … Contact person's name, position and contact details: … Description of the processing: …	Name: … Address: … Contact person's name, position and contact details: … Description of the processing: …
Name: … Address: … Contact person's name, position and contact details: … Description of the processing: …	Name: … Address: … Contact person's name, position and contact details: … Description of the processing: …
Name: … Address: … Contact person's name, position and contact details: … Description of the processing: …	Name: … Address: … Contact person's name, position and contact details: … Description of the processing: …

ANNEX II: STANDARD CONTRACTUAL CLAUSES

This annex applies if the Sub-Processor is a company located outside the EEA, in a third-country not subject to an adequacy decision by the European Commission.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation)1 for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Appendix 1. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Appendix 1. (hereinafter each "data importer")

(iii) have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Appendix 2.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(e) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(f) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

- (i) Clause 1, Clause 2, Clause 3, Clause 6 ;
- (ii) Clause 7.1(a), (c) and (d) and Clause 7.9(a), (c), (d), (e), (f) and (g) ;
- (iii) Clause 8(a), (c), (d) and (e) ;
- (iv) Clause 11(a), (d) and (f);
- (v) Clause 12;
- (vi) Clause 14.1(c), (d) and (e);
- (vii) Clause 15 e);
- (viii) Clause 17(a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(c) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(d) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(e) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Appendix 2.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 7

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

7.1 Instructions

(f) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(g) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The

controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(h) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(i) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

7.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Appendix 2, unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

7.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

7.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

7.5 Duration of processing and erasure or return of Data

Processing by the data importer shall only take place for the duration specified in Annex I.A. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 13, in particular the requirement for the data importer under Clause 13(e) to notify

the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 13(a).

7.6 Security of processing

(j) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex I.B. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(k) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(l) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(m) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

7.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to

criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

7.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

7.9 Documentation and compliance

(n) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(o) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(p) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(q) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(r) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(s) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(t) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 8

Use of sub-processors

(u) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub- processors at least one month in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(v) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 7.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(w) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(x) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub- processor to fulfil its obligations under that contract.

(y) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 9

Data subject rights

(z) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(aa) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex I.B the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(bb) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter

Clause 10

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

  (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 12;

  (ii) refer the dispute to the competent courts within the meaning of Clause 17.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 11

Liability

(g) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(h) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(i) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(j) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(k) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(l) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(m) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 12

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.A, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.A, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.A, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 13

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(iii) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(iv) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(v) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by

the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 15(d) and (e) shall apply.

Clause 14

Obligations of the data importer in case of access by public authorities

14.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(vi) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(vii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

The data exporter shall forward the notification to the controller.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the notification to the controller.

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 13(e) and Clause 15 to inform the data exporter promptly where it is unable to comply with these Clauses.

14.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful

assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 13(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 15

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 13(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(viii) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ix) the data importer is in substantial or persistent breach of these Clauses; or

(x) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority and the controller of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter.

Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 16

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (specify Member State).

Clause 17

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of _____ (specify Member State).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

1. List of Parties

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: Please specify the mci group entity
Address: ...
Contact person's name, position and contact details: Anne Lesca, DPO, privacy@mci-group.com
Activities relevant to the data transferred under these Clauses: ...
Signature and date: ...
Role (data processor/sub-processor): ...

2 ...
...

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: ...
Address: ...
Contact person's name, position and contact details: ...
Activities relevant to the data transferred under these Clauses: ...
Signature and date: ...
Role (data processor/sub-processor): ...

2.
...

2. Description of Transfer

Categories of data subjects whose personal data is transferred

.....

Categories of personal data transferred

.....

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

.....

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

.....

Nature of the processing

.....

Purpose(s) of the data transfer and further processing

.....

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

.....

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

.....