Interaffiliate Data Processing and Transfer Agreement

This Interaffiliate Data Processing and Transfer Agreement (together with any appendices attached hereto, the "**Agreement**") is entered into between the affiliates identified in the signature pages as parties to this Agreement (individually and collectively, "**Company**").

WHEREAS The purpose of this Agreement is to regulate the Processing of Personal Data, if any, between the Company to this Agreement as well as the transfer or disclosure of Personal Data as defined herein.

1. DEFINITIONS

For the purposes of this Agreement:

1.1. "**Data Controller**" means any Company entity that determines the purposes and means of Processing.

1.2. "**Data Exporter**" means any Company entity settled in the EEA that discloses or transfers Personal Information to a Data Importer. The Data Exporter may be Data Controller or Data Processor.

1.3. "**Data Importer**" means any Company entity settled out of the EEA that receives or accesses Personal Information from a Data Exporter.

1.4. "**Data Processor**" means any entity (other than the Data Controller) that Processes Personal Information on the Data Controller's behalf.

1.5. "**Data Subject**" or "**Individual**" means any individual about whom Personal Information may be Processed.

1.6. "**Identifiable"** means who can be, directly or indirectly, in particular by reference to an identifier such as name, location data, identification number or by any other factor as Sensitive Information.

1.7. "**Personal Information**" or "**Personal Data**" means any information that identifies an individual or relates to an Identifiable individual and is received from another party under this Agreement.

1.8. "**Process**" or "**Processing**" means the collection, recording, organization, structuring, alteration, use, access, disclosure, copying, transfer, storage, deletion, combination, restriction, adaptation, retrieval, consultation, destruction, disposal or other use of Personal Information, whether or not by automated means.

1.9. "**Recipient**" means the legal person to which the Personal Information are disclosed, whether a third party or not.

1.10. "**Special Categories of Data**" or "**Sensitive Information**" means any of the following types of Personal Information: (i) social security number, taxpayer identification number, passport number, driver's license number or other government-issued identification number; (ii) credit or debit card details or financial account number, with or without any code or password that would permit access to the account, and credit history; or (iii) information on race, religion, ethnicity, sex life or practices or sexual orientation, medical or health information, genetic or biometric information, biometric templates, political or philosophical beliefs, political party or trade union membership, background check information, judicial data such as criminal records or information on other judicial or administrative proceedings.

2. DATA PROTECTION PRINCIPLES

Data Importer will:

2.1. Process Personal Information consistent with the specific, legitimate and lawful purposes described in the attached Description of Transfer (Exhibit A), which reflects the purposes set forth in any applicable privacy notices made available by Data Exporter or Data Controller to Individuals.

2.2. Keep the Personal Information accurate and up-to-date for the intended Processing purposes.

2.3. Process only Personal Information that is relevant and required for the intended Processing purposes, unless otherwise permitted by applicable law.

2.4. Retain Personal Information only as long as necessary and consistent with the purpose for which it was collected or Processed.

2.5. Limit access to Personal Information to Individuals who have a legitimate business need to access the Personal Information for the intended Processing purposes.

2.6. Develop, implement, maintain, monitor, and, where necessary, update a comprehensive written information security program that contains appropriate and reasonable administrative, technical, physical and organizational safeguards, including those described in the attached Security Standards (Exhibit B), to protect Personal Information against Security Incidents (as defined at Section 3.7) and unauthorized Processing and to provide a level of commensurate security with the risks posed by Processing the Personal Information ("**Information Security Program**").

3. ADDITIONAL DATA PROCESSOR TERMS

Where a Data Importer is acting as a Data Processor, the Data Importer also will comply with the following requirements, in accordance with the article 28 of the General Data Protection Regulation ("**GDPR**") and the basic principles of the GDPR in Chapter II:

3.1. Limitations on Use. Data Importer will Process Personal Information only in accordance with Data Controller's documented instructions, which may be provided in written or electronic form, or, if not available, at least consistent with the scope, classification, purposes and details of Processing described in the attached Description of Transfer. The duration of the Processing will be the same as the period during which this Agreement is in effect, except as otherwise agreed by Data Controller and Data Importer.

3.2. Confidentiality. Data Importer will hold Personal Information in strict confidence and impose confidentiality obligations on personnel who will be provided access to or will otherwise Process Personal Information, including to protect all Personal Information consistent with the requirements of this Agreement (including during the term of their employment or engagement and thereafter).

3.3. Data Integrity. Data Importer will ensure that all Personal Information Processed by Data Importer on Data Controller's behalf is accurate and kept up to date and that any Personal Information that is inaccurate or incomplete is erased or rectified in accordance with Data Controller's instructions.

3.4. Requests or Complaints from Individuals. Data Importer will promptly notify Data Controller, unless specifically prohibited by laws applicable to Data Importer, if Data Importer receives: (i) any requests from an Individual with respect to Personal Information Processed, including but not limited to opt-out requests, requests for access and/or rectification, erasure, restriction, requests for data portability and all similar requests; or (ii) any complaint relating to Personal Information Processing, including allegations that the Processing infringes on an Individual's rights. Data Importer will not respond to any such request or complaint unless expressly authorized to do so by Data Controller, will cooperate with Data Controller with respect to any action taken relating to such request or complaint and will seek to implement appropriate processes (including technical and organizational measures) to assist Data Controller in responding to requests or complaints from Individuals.

3.5. Disclosure Requests. If Data Importer receives any order, demand, warrant or any other document requesting or purporting requiring the production of Personal Information (including, for example, by oral questions, interrogatories, requests for information or documents in legal proceedings, subpoenas, civil investigative demands or other similar processes) ("**Disclosure Request**"), Data Importer will without undue delay notify Data Controller (except to the extent otherwise required by laws applicable to Data Importer) and will cooperate with Data Controller with respect to any action taken with respect to such Disclosure Request.

3.6. Audit. Data Importer will provide to Data Controller, its authorized representatives and such independent inspection body as Data Controller may appoint, on reasonable notice: (i) access to Data Importer's information, processing premises and records; (ii) reasonable assistance and cooperation of Data Importer's relevant staff; and (iii) reasonable facilities at Data Importer's premises for the purpose of auditing Data Importer's compliance with its obligations under this Agreement.

3.7. Security Incident. Data Importer will, within thirty-six (36) hours, notify Data Controller whenever Data Importer reasonably believes that there has been any accidental or unauthorized access, acquisition, use, modification, disclosure, loss, damage or destruction of Personal Information ("**Security Incident**"). This notification shall describe the nature of the Security Incident and precise any information to enable the Data Controller to notify, if necessary, this Security Incident to the supervisory authority competent, to investigate Security Incident and to take reasonable measures and appropriate corrective actions e.g. to remedy the Security Incident and / or to avoid/prevent further loss or damages arising therefrom. Data Importer will cooperate in investigating, containing, correcting and remediating the Security Incident and any resulting damage, including assisting with any notifications to affected Individuals, regulators and third parties that Data Controller deems appropriate.

3.8. Return or Disposal. Upon termination or expiration of this Agreement for any reason or upon Data Controller's request, Data Importer will immediately cease handling Personal Information and will return in a manner and format reasonably requested by Data Controller, or, if specifically directed by Data Controller, will destroy, any or all Data Controller Information in Data Importer's possession, power or control, except as otherwise required by law applicable to Data Importer. If Data Importer has such a legal obligation to retain Personal Information beyond the period otherwise specified by this Section, Data Importer will return or destroy the Personal Information in accordance with this Section as soon as possible after that legally required retention period has ended.

3.9. Other. Data Importer will take any other steps reasonably requested by Data Controller, in particular in order to assist Data Controller in meeting its obligations under data protection laws regarding (i) registration and notification, (ii) accountability, (iii) maintaining the security of the Personal Information and (iv) performance of privacy and data protection impact assessments and related consultations with data protection authorities. Data Importer will inform Data Controller if Data Importer believes that any instructions of Data Controller regarding the Processing of Personal Information would violate applicable law.

3.10. Adverse Changes. Data Importer will notify Data Controller promptly if Data Importer: (i) has reason to believe that it is unable to comply with any of its obligations under this Agreement and it cannot cure this inability to comply within a reasonable timeframe; or (ii) becomes aware of any circumstances or change in applicable law that is likely to prevent it from fulfilling its obligations under this Agreement. In the event that this Agreement does not or would not, or any actions to be taken or contemplated to be taken in performance of this Agreement do not or would not, satisfy either party's obligations under the laws applicable to each party, the parties will negotiate in good faith upon an appropriate amendment to this Agreement.

4. DATA TRANSFERS

4.1. Restricted Transfers from EEA. This Section 4.1 applies solely when a Data Exporter located in a Member State of the European Economic Area ("**EEA**") (an "**EEA Country**") transfers or discloses Personal Information to a Data Importer in a location other than the EEA Country.

4.1.1. Such transfers will be governed by the attached EU Standard Contractual Clauses as set out below and each concerned Party hereof accepts hereby the application of the appropriate EU Standard Contractual Clauses where needed by singing this Agreement, unless (i) the transfer is to a Data Importer covered by an adequacy decision adopted by the European Commission under article 45 of GDPR (including Privacy Shield and any successor program) or (ii) where Data Importer acts as Data Processor, Data Importer has implemented and is bound by Binding Corporate Rules in all jurisdictions where Personal Information will be transferred and Processed.

4.1.2. If the transfer is to a Data Importer acting as a Data Controller, the transfer will be governed by the attached Standard Contractual Clauses (Controller to Controller) (Commission decision 2004/915/EC of 27 December 2004) (Exhibit C), together with the EU Data Processing Principles and the Description of Transfer.

4.1.3. If the transfer is to a Data Importer acting as a Data Processor, the transfer will be governed by the attached Standard Contractual Clauses (Controller to Processor) (Commission decision 2010/87/EU of 5 February 2010) (Exhibit D), together with the attached Description of Transfer and the Security Standards.

4.1.4. If the transfer is to a Data Importer acting a Recipient, the transfer will be also governed by the attached Standard Contractual Clauses (Controller to Processor) (Commission decision 2010/87/EU of 5 February 2010) (Exhibit D), together with the attached Description of Transfer and the Security Standards.

4.2. For avoidance of doubt, Data Importer must continue to comply with its general obligations under Sections 1-7 of this Agreement, and in addition to Sections 4.1-4.2, where applicable.

5. SUBCONTRACTING

5.1. Data Importer may disclose or transfer Personal Information to a Data Processor that is not a party to this Agreement, provided that Data Importer impose obligations in writing upon the Data Processor that are compliant with article 28 of GDPR. However, Data Importer remains liable towards the Data Exporter in case third party Data Processor fails to comply with such imposed data protection obligations.

5.2. In addition, where Data Importer is acting as a Data Processor, Data Importer has the right to engage another processor to act as sub-processor. In this case, Data Importer shall inform, in writing and without delay, the Data Controller of any designation, addition or replacement of a sub-processor. This information shall indicate the Processed activities, the name and the contact details of the sub-processors and the duration of the subcontract. The Data Controller shall have a period of fifteen (15) days from the reception of this information to object to such changes. The sub-processor is deemed accepted if the Data Controller does not objet within this time.

6. TERM AND TERMINATION

6.1. This Agreement will be effective as of May 25, 2018 ("**Effective Date**"), unless specified differently with respect to a particular Company entity on its signature page.

6.2. Any Company may at any time terminate its status as a party to this Agreement, in whole or in part, with respect to any or all parties to this Agreement. Such termination will take immediate effect upon the submission in writing of notice to the relevant parties hereunder.

6.3. However, where a Company exercises the right to terminate its status as a party to this Agreement, such termination will not affect the obligations imposed on parties (including the terminating Company) under applicable provisions of Sections 2, 3, 4, and 5 of this Agreement with respect to Personal Information disclosed or transferred prior to the termination of this Agreement.

7. MISCELLANEOUS

7.1. The construction, validity and performance of this Agreement will be governed by the laws of France, unless other mandatory national laws apply. Each party submits to the jurisdiction of the competent courts of Paris for the purposes of determining any dispute arising out of this Agreement.

7.2. To the extent there is any conflict between Sections 1-7 of this Agreement and the terms of the Standard Contractual Clauses, the Standard Contractual Clauses prevail.

7.3. This Agreement may be executed in several counterparts (including delivery via facsimile or electronic mail), each of which will be deemed to be an original but all of which together will constitute one and the same instrument.

7.4. This Agreement is not intended to confer any rights upon any person or entity not subject to this Agreement other than as specifically provided for in this Agreement.

7.5. This Agreement supersedes and replaces any prior agreements concerning the same subject matter.

7.6. Counterparts.

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

IN WITNESS WHEREOF, each of the undersigned companies has caused this Interaffiliate Data Processing and Transfer Agreement to be signed and delivered by its duly authorized representative.

[Signature pages follow]

Dated:

Data Exporter and Data Importer

CONSTELLIUM N.V.

By: _____

Name(s): _____

Title: _____

CONSTELLIUM HOLDCO II B.V.

By: _____

Name(s): _____

Title: _____

CONSTELLIUM N.V. (French branch)

By: _____

Name(s): _____

Title: _____

CONSTELLIUM INTERNATIONAL

By: _____

Name(s): _____

Title: _____

CONSTELLIUM FINANCE

By: _____

Name(s): _____

Title: _____

CONSTELLIUM FRANCE HOLDCO

By: _____

Name(s): _____

Title: _____

CONSTELLIUM USSEL

By: _____

Name(s): _____

Title: _____

CONSTELLIUM EXTRUSION FRANCE

By: _____

Name(s): _____

Title: _____

CONSTELLIUM PARIS

By: _____

Name(s): _____

Title: _____

C-TEC CONSTELLIUM TECHNOLOGY CENTER

By: _____

Name(s): _____

Title: _____

CONSTELLIUM NEUF-BRISACH

By: _____

Name(s): _____

Title: _____

CONSTELLIUM ISSOIRE

By: _____

Name(s): _____

Title: _____

CONSTELLIUM MONTREUIL-JUIGNÊ

By: _____

Name(s): _____

Title: _____

CONSTELLIUM FRANCE III

By: _____

Name(s): _____

Title: _____

ENGINEERED PRODUCTS INTERNATIONAL

By: _____

Name(s): _____

Title: _____

CONSTELLIUM SINGEN GMBH

By: _____

Name(s): _____

Title: _____

CONSTELLIUM DEUTSCHLAND GMBH

By: _____

Name(s): _____

Title: _____

CONSTELLIUM ROLLED PRODUCTS SINGEN GMBH & Co. KG
represented by its general partner
CONSTELLIUM SINGEN GMBH

By: _____

Name(s): _____

Title: _____

CONSTELLIUM GERMANY HOLDCO GMBH & Co. KG
represented by its general partner
CONSTELLIUM GERMANY VERWALTUNGS GMBH

By: _____

Name(s): _____

Title: _____

CONSTELLIUM GERMANY VERWALTUNGS GMBH

By: _____

Name(s): _____

Title: _____

CONSTELLIUM TREUHAND UG (HAFTUNGSBESCHRÄNKT)

By: _____

Name(s): _____

Title: _____

CONSTELLIUM EXTRUSIONS LANDAU GMBH

By: _____

Name(s): _____

Title: _____

CONSTELLIUM EXTRUSIONS DEUTSCHLAND GMBH

By: _____

Name(s): _____

Title: _____

CONSTELLIUM EXTRUSIONS BURG GMBH

By: _____

Name(s): _____

Title: _____

CONSTELLIUM AUTOMOTIVE ZILINA S.R.O.

By: _____

Name(s): _____

Title: _____

CONSTELLIUM EXTRUSIONS DECIN S.R.O.

By: _____

Name(s): _____

Title: _____

CONSTELLIUM EXTRUSIONS LEVICE S.R.O.

By: _____

Name(s): _____

Title: _____

CONSTELLIUM UK LIMITED

By: _____

Name(s): _____

Title: _____

CONSTELLIUM VALAIS SA

By: _____

Name(s): _____

Title: _____

CONSTELLIUM SWITZERLAND AG

By: _____

Name(s): _____

Title: _____

CONSTELLIUM ITALY S.P.A.

By: _____

Name(s): _____

Title: _____

CONSTELLIUM W

By: _____

Name(s): _____

Title: _____

CONSTELLIUM HOLDINGS MUSCLE SHOALS LLC

By: _____

Name(s): _____

Title: _____

CONSTELLIUM MUSCLE SHOALS LLC

By: _____

Name(s): _____

Title: _____

CONSTELLIUM MUSCLE SHOALS FUNDING II LLC

By: _____

Name(s): _____

Title: _____

LISTERHILL TOTAL MAINTENCNANCE CENTER LLC

By: _____

Name(s): _____

Title: _____

CONSTELLIUM US HOLDINGS I, LLC

By: _____

Name(s): _____

Title: _____

CONSTELLIUM AUTOMOTIVE USA, LLC

By: _____

Name(s): _____

Title: _____

CONSTELLIUM ROLLED PRODUCTS RAVENSWOOD, LLC

By: _____

Name(s): _____

Title: _____

CONSTELLIUM-UACJ ABS LLC

By: _____

Name(s): _____

Title: _____

CONSTELLIUM METAL PROCUREMENT LLC

By: _____

Name(s): _____

Title: _____

CONSTELLIUM PROPERTY AND EQUIPMENT COMPANY LLC

By: _____

Name(s): _____

Title: _____

CONSTELLIUM AUTOMOTIVE MÉXICO TRADING, S. DE E.L. DE C.V.

By: _____

Name(s): _____

Title: _____

CONSTELLIUM AUTOMOTIVE MÉXICO, S. DE R.L. DE C.V.

By: _____

Name(s): _____

Title: _____

CONSTELLIUM AUTOMOTIVE MÉXICO TRADING, S. DE E.L. DE C.V.

By: _____

Name(s): _____

Title: _____

CONSTELLIUM SOUTHEAST ASIA PTE. LTD.

By: _____

Name(s): _____

Title: _____

CONSTELLIUM JAPAN K.K.

By: _____

Name(s): _____

Title: _____

CONSTELLIUM ENGLEY (CHANGCHUN) AUTOMOTIVE STRUCTURES Co. LTD.

By: _____

Name(s): _____

Title: _____

CONSTELLIUM CHINA

By: _____

Name(s): _____

Title: _____

EXHIBIT A

Description of Transfer re: HR Data

Data subjects:

The personal data transferred concern the following categories of data subjects:

- **Past and present employees and non-employee workers.**
- **Past and present advisers, consultants, independent contractors, agents and other professional experts, and autonomous, temporary or casual workers.**
- **Students, interns, apprentices and volunteers.**
- **Job applicants and candidates.**
- **Past and present directors and officers.**
- **Retirees.**
- **Individuals identified by the aforementioned Data Subjects as beneficiaries, domestic partners, family members and emergency contacts.**

Categories of data:

The personal data transferred concern the following categories of data:

- **Personal Details: Name, maiden name and surname; e-mail and telephone details; home address; birth date; national identification number; gender; marital status; dependents; emergency contact information; photograph.**
- **Documentation Required Under Immigration Laws: Citizenship; passport data; details of residency or work permit.**
- **Payroll Data: Banking details, working time records (including vacation and other absence records, leave status, hours worked and department standard hours) and termination date.**
- **Position: Description of current position; title; salary plan; pay grade or level; unit/department; location; supervisor(s) and subordinate(s); Company contact(s); employee identification number or Company assigned number; employment or contract status and type; terms of employment or contract; employment contract; work history with Company; (re-)hire and termination date(s), length of service, retirement eligibility, promotions and disciplinary records.**
- **Talent Management Information: Details contained in letters of application and resume/CV; previous employment or work background; education history; professional qualifications; language and other relevant skills; details on performance management ratings; development plan and willingness to relocate.**
- **Compensation: Base salary; bonus; benefits; pay enhancements for dependents; overtime and shift work; salary step within assigned grade; details on stock options; stock grants and other awards; currency; pay frequency; effective date of current compensation; salary reviews and performance appraisals; compensation details.**

- **Management Records: Details of any shares of common stock or directorships.**

- **System and Application Access Data: Information required to access company systems and applications such as user IDs for Company network or servers, email account, instant messaging account, passwords, access logs, activity logs, and electronic content produced by Data Subjects using company systems.**

Sensitive data:

The personal data transferred concern the following categories of sensitive data:

Sensitive Data as required and permitted by laws applicable to the transfer: For example, personal data that identify health-related conditions, such as where required for making an accommodation or processing absence requests or insurance claims; church or religious affiliation where required for statutory tax deductions or to accommodate meal or other requests; membership in union or work council and diversity-related personal data (such as sex and racial or ethnic origin) in order to comply with legal obligations and internal policies relating to diversity and anti-discrimination; and information necessary to perform background checks where applicable.

Recipients:

The personal data transferred may be disclosed to the following recipients or categories of recipients:

- **Managers and their designees; and**

- **Authorized personnel in HR, IT, Finance, Tax, Legal, Procurement, Compliance and Audit departments.**

All personnel within Company will generally have access to business contact information such as name, position, workplace telephone numbers, addresses and email addresses.

Purposes of the transfer / Processing operations:

The transfer is made for the following purposes. If Data Importer functions only as a data processor and does not function as a data controller, the personal data will be subject to processing activities that support the Data Exporter in achieving the following purposes:

- **Managing Workforce: Managing work activities and personnel generally, including evaluations, promotions and succession planning; administering and paying salary and wages; conducting reviews; administering awards such as stock options, stock grants and bonuses; managing health care, pensions and savings plans; managing and administering training, leave, promotions, transfers and secondments; honoring other contractual benefits; organizing recreational activities; granting loans; performing workforce analysis and planning and background checks; managing coaching, disciplinary matters and terminations; and making business travel arrangements.**

- **Communications and Emergencies: Facilitating communication with data subjects, including in an emergency; providing references and recommendations; protecting the health and safety of employees and others; and safeguarding IT infrastructure, office equipment and other property.**

- **Business Operations: Operating and managing the IT and communications systems, including provision and support of network, data, telecom and other IT infrastructure, application hosting, data storage, backup and restore, messaging and collaboration applications, middleware applications, end user services (e.g., desktop and mobile computing and remote access), IT security operations, and related development, support and maintenance services; managing product and service development; improving products and services; managing Company assets; allocating Company assets and human resources; conducting strategic planning and project management; ensuring business continuity and disaster recovery; compiling audit trails and other reporting tools; maintaining records relating to manufacturing and other business activities; conducting budgeting, financial management and reporting; ensuring communications; and managing mergers, acquisitions and re-organizations or disposals.**

- **Compliance: (i) Complying with legal and other requirements, such as income tax and national insurance deductions; recordkeeping and reporting obligations; conducting audits; facilitating compliance with government inspections and responding to other requests from government or other public authorities; responding to legal process such as subpoenas; pursuing legal rights and remedies; defending litigation and managing any internal complaints or claims, conducting internal investigations; and complying with internal policies and procedures; (ii) protecting, enforcing or defending the legal rights, privacy, safety, or property of Company, Company affiliates or their employees, agents and contractors (including enforcement of relevant agreements and terms of use); (iii) protecting the safety, privacy, and security of users of Company products or services or members of the public; or (iv) protecting against fraud or for risk management purposes.**

- **Employee Resource Usage and Corporate Investigations: Monitoring activities as permitted by local law (including monitoring telephone, email, Internet and other Company resources); and conducting internal investigations.**

Description of Transfer re: Customer, Supplier and / or Cooperation Partner Data

Data subjects:

The personal data transferred concern the following categories of data subjects:

- Existing and prospective clients and customers, including without limitation corporate customers' employees, directors and officers.

- Existing and prospective suppliers and cooperation partners (private or public) including without limitation corporate suppliers' employees, directors and officers.

Categories of data:

The personal data transferred concern the following categories of data:

- **Personal Details and Contact Information:** Name; address; e-mail; telephone and fax details and other contact information; photograph, voice recordings and video; signature and electronic signature.
- **Professional Affiliations:** Business name, title and address.
- **Financial Information:** Payment card number; bank account number and account details; tax returns; salary; assets and income; personal bankruptcy; credit history and credit score.
- **Marketing Preferences and Customer Service Interactions:** Marketing preferences; entry in contest or promotion; responses to voluntary surveys; and recordings of telephone calls with customer service and other representatives.
- **Operational Data:** Transactions, sales, purchases, product registration information, uses, supplier information, credentials to online services and platforms, and electronic content produced by data subjects using Company systems, including online interactive and voice communications such as blogs, chat, webcam use and network sessions.
- **Connected Data:** Data collected by Company from appliances and smart devices used to access Company's WiFi applications.

Sensitive data:

The personal data transferred concern the following categories of sensitive data:

- Only sensitive data as may be relevant for a customer or supplier relationship.
- Special categories of data may be collected, used and transferred to the extent needed to comply with applicable laws and regulations or based on explicit consent from the data subject.

Recipients:

The personal data transferred may be disclosed to the following recipients or categories of recipients:

- Authorized personnel in Sales, Marketing, IT, Legal, Tax, Finance, Procurement, Technology and Audit departments.

Purposes of the transfer / Processing operations

The transfer is made for the following purposes. If Data Importer functions only as a data processor and does not function as a data controller, the personal data will be subject to processing activities that support the Data Exporter in achieving the following purposes:

- **Communications:** Facilitating communication with customers / suppliers / private and/or public cooperation partners and responding to individuals' reports, reviews, correspondence or enquiry regarding Company products and services; providing and improving customer services; marketing products and services to data subjects; and facilitating communications generally in the context of business activities concerning the preparation, establishment, execution and termination of the construal business relationship.
- **Business Operations:** Providing products and services to customers; operating and managing the IT and communications systems; marketing Company's or our business partners' products and services; managing product and service development; improving our products and services; managing company assets; allocating Company assets and human resources; strategic planning; project management; business continuity; disaster recovery; compilation of audit trails and other reporting tools; maintaining records relating to manufacturing and other business activities; budgeting; financial management and reporting; communications within and outside group of companies; managing acquisitions, mergers and re-organizations or sale of a company.
- **Compliance:** (i) Complying with legal and other requirements, such as income tax and national insurance deductions; recordkeeping and reporting obligations; conducting audits; facilitating compliance with government inspections and responding to other requests from government or other public authorities; responding to legal process such as subpoenas; pursuing legal rights and remedies; defending litigation and managing any internal complaints or claims, conducting internal investigations; and complying with internal policies and procedures; (ii) protecting, enforcing or defending the legal rights, privacy, safety, or property of Company, Company affiliates or their employees, agents and contractors (including enforcement of relevant agreements and terms of use); (iii) protecting the safety, privacy, and security of users of Company products or services or members of the public; or (iv) protecting against fraud or for risk management purposes.

EXHIBIT B

Security Standards

Data Importer maintains and enforces various policies, standards and processes designed to secure Personal Data and other data to which Data Importer employees are provided access. Following is a description of some of the core technical and organizational security measures implemented by Data Importer.

This appendix represents the minimum security measures that will be taken by Data Importer:

1. Information Security Policies and Standards

The Data Importer will implement security requirements for staff and all subcontractors, vendors or agents who have access to Personal Data that are designed to:

1. Prevent unauthorized persons from gaining access to Personal Data processing systems (physical access control);

2. Prevent Personal Data processing systems from being used without authorization (logical access control);

3. Ensure that persons entitled to use a Personal Data processing system gain access only to such Personal Data as they are entitled to access in accordance with their access rights and that, in the course of Processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorization (data access control);

4. Ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control);

5. Ensure the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in or removed from Personal Data Processing (entry control);

6. Ensure that Personal Data are Processed solely in accordance with the Instructions of the Data Controller (control of instructions);

7. Ensure that Personal Data are protected against accidental destruction or loss (availability control); and

8. Ensure that Personal Data collected for different purposes can be processed separately (separation control).

Data Importer will conduct periodic risk assessments and review and, as appropriate, revise its information security practices at least annually or whenever there is a material change in Data Importer's business practices that may reasonably affect the security, confidentiality or integrity of Personal Information, provided that Data Importer will not modify its information security practices in a manner that will weaken or compromise the confidentiality, availability or integrity of Personal Information.

2. Physical Security

The Data Importer will maintain commercially reasonable security systems at all Data Importer sites at which an information system that uses or houses Personal Data is located. The Data Importer reasonably restricts access to such Personal Data appropriately.

3. Organizational Security

When media (for example copy machines, laptops, etc.) are to be disposed of or reused, procedures have been implemented to prevent any subsequent retrieval of any Personal Data stored on them before they are withdrawn from the inventory. When media are to leave the premises at which the files are located as a result of maintenance operations, procedures have been implemented to prevent undue retrieval of Personal Data stored on them.

Data Importer will implement security policies and procedures to classify personal and sensitive data, clarify security responsibilities and promote awareness for employees.

All Personal Data security incidents are managed in accordance with appropriate incident response procedures.

4. Network Security

The Data Importer maintains network security using commercially available equipment and industry standard techniques, including firewalls, intrusion detection and/or prevention systems, access control lists and routing protocols.

5. Access Control

Data Importer will maintain appropriate access controls, including, but not limited to, restricting access to Personal Information to the minimum number of Data Importer personnel who require such access.

Only authorized staff can grant, modify or revoke access to an information system that uses or houses Personal Information.

User administration procedures define user roles and their privileges, and how access is granted, changed and terminated; address appropriate segregation of duties and define the logging/monitoring requirements and mechanisms.

All employees of the Data Importer are assigned unique User-IDs.

Access rights are implemented adhering to the “least privilege” approach.

Data Importer implements commercially reasonable physical and electronic security to create and protect passwords.

6. Encryption

Data Importer will encrypt, using industry-standard encryption tools, all sensitive data that Data Importer: (i) transmits or sends wirelessly or across public networks; (ii) stores on laptops or storage media; and (iii) stores on portable devices, where technically feasible. Data Importer will safeguard the security and confidentiality of all encryption keys associated with encrypted Sensitive Information.

7. **Virus and Malware Controls**

The Data Importer installs and maintains anti-virus and malware protection software on the system to protect Personal Information from anticipated threats or hazards and protect against unauthorized access to or use of Personal Information.

8. **Personnel**

Data Importer will require personnel to comply with its Information Security Program prior to providing personnel with access to Personal Information.

The Data Importer implements a security awareness program to train personnel about their security obligations. This program includes training about data classification obligations; physical security controls; security practices and security incident reporting.

9. **Business Continuity**

The Data Importer implements appropriate disaster recovery and business continuity plans. Data Importer regularly reviews and updates its business continuity plan to ensure it is current and effective.

10. **Primary Security Manager**

Data Importer will notify Data Exporter of its designated primary security manager upon request. The security manager will be responsible for managing and coordinating the performance of Data Importer's obligations set forth in its Information Security Program and in this Agreement.

EXHIBIT C

Standard contractual clauses for the transfer of personal data to third countries (Controller to Controller; Commission decision 2004/915/EC of 27 December 2004): SET II

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

Data transfer agreement

between

Name: _____

Address and country of establishment: _____

_____

(hereinafter "data exporter")

and

Name: _____

Address and country of establishment: _____

_____

(hereinafter "data importer"

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

Definitions

For the purposes of the clauses:

(a) "*personal data*", "*special categories of data/sensitive data*", "*process/processing*", "*controller*", "*processor*", "*data subject*" and "*supervisory authority/authority*" shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby "*the authority*" shall mean the competent data protection authority in the territory in which the data exporter is established);

(b) "*the data exporter*" shall mean the controller who transfers the personal data;

(c) "*the data importer*" shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection;

(d) "*clauses*" shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. Obligations of the data exporter

The data exporter warrants and undertakes that:

(a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

(b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

(c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

(d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

(e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

(a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

(b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

(c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

(d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

(e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

(f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

(g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

(h) It will process the personal data, at its option, in accordance with:

(i) the data protection laws of the country in which the data exporter is established, or

(ii) the relevant provisions[1] of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data[2], or

(iii) the data processing principles set forth in Annex A.

Data importer to indicate which option it selects: _____

_____

Initials of data importer:_____

_____;

(i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

(i) the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

(ii) the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

(iii) data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

(iv) with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer.

III. Liability and third party rights

(a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

(b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data

---

1 "Relevant provisions" means those provisions of any authorisation or decision except for the enforcement provisions of any authorisation or decision (which shall be governed by these clauses)

2 However, the provisions of Annex A.5 concerning the rights of access, rectification, deletion and objection must be applied when this option is chosen and take precedence over any comparable provisions of the Commission Decision selected.

exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

(a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

(b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

(c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. Termination

(a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

(b) In the event that:

(i) the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

(ii) compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

(iii) the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

(iv) a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

(v) a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

(c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector

thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

(d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

Dated: _____

On behalf of the data exporter:

Name (written out in full): _____

Position: _____

Address: _____

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

_____

Signature…….

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): _____

Position: _____

Address: _____

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

_____

Signature…….

(stamp of organisation)

ANNEX A

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to “opt-out” from having his data used for such purposes.

8. Automated decisions: For purposes hereof “automated decision” shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

(a)(i)such decisions are made by the data importer in entering into or performing a contract with the data subject, and

(ii)(the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

or

(b) where otherwise provided by the law of the data exporter.

ANNEX B

DESCRIPTION OF THE TRANSFER

(To be completed by the parties)

Data subjects

The personal data transferred concern the following categories of data subjects:

.....

.....

.....

.....

Purposes of the transfer(s)

The transfer is made for the following purposes:

.....

.....

.....

.....

Categories of data

The personal data transferred concern the following categories of data:

.....

.....

.....

.....

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients:

.....

.....

.....

Sensitive data (if appropriate)

The personal data transferred concern the following categories of sensitive data:

.....

.....

.....

.....

Data protection registration information of data exporter (where applicable)

.....

.....

Additional useful information (storage limits and other relevant information)

.....

.....

Contact points for data protection enquiries

Data importer	**Data exporter**
.....	.....
.....	.....
.....	.....

ILLUSTRATIVE COMMERCIAL CLAUSES (OPTIONAL)

Indemnification between the data exporter and data importer:

"The parties will indemnify each other and hold each other harmless from any cost, charge, damages, expense or loss which they cause each other as a result of their breach of any of the provisions of these clauses. Indemnification hereunder is contingent upon (a) the party(ies) to be indemnified (the "indemnified party(ies)") promptly notifying the other party(ies) (the "indemnifying party(ies)") of a claim, (b) the indemnifying party(ies) having sole control of the defence and settlement of any such claim, and (c) the indemnified party(ies) providing reasonable cooperation and assistance to the indemnifying party(ies) in defence of such claim.".

Dispute resolution between the data exporter and data importer (the parties may of course substitute any other alternative dispute resolution or jurisdictional clause):

"In the event of a dispute between the data importer and the data exporter concerning any alleged breach of any provision of these clauses, such dispute shall be finally settled under the rules of arbitration of the International Chamber of Commerce by one or more arbitrators appointed in accordance with the said rules. The place of arbitration shall be [ ]. The number of arbitrators shall be [ ]."

Allocation of costs:

"Each party shall perform its obligations under these clauses at its own cost."

Extra termination clause:

"In the event of termination of these clauses, the data importer must return all personal data and all copies of the personal data subject to these clauses to the data exporter forthwith or, at the data exporter's choice, will destroy all copies of the same and certify to the data exporter that it has done so, unless the data importer is prevented by its national law or local regulator from destroying or returning all or part of such data, in which event the data will be kept confidential and will not be actively processed for any purpose. The data importer agrees that, if so requested by the data exporter, it will allow the data exporter, or an inspection agent selected by the data exporter and not reasonably objected to by the data importer, access to its establishment to verify that this has been done, with reasonable notice and during business hours.

EXHIBIT D

Standard contractual clauses for the transfer of personal data to third countries (Controller to Processor; Commission decision 2010/87/EU of 5 February 2010)

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

Name of the data exporting organisation: _____

Address: _____

Tel.:_____; Fax: _____; E-Mail: _____

Other information needed to identify the organisation:

_____

(the data **exporter**)

and

Name of the data importing organisation: _____

Address: _____

Tel.:_____; Fax: _____; E-Mail: _____

Other information needed to identify the organisation:

_____

(the data **importer**)

each a “party”; together “the parties”,

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

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[3];

(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

---

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

the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

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

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

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

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

Clause 5

Obligations of the data importer[4]

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;

---

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

(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 or 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 state in which the data exporter is established, namely _____.

Clause 10

Variation of the contract

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

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[5]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

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

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

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

---

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

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full): _____

Position: _____

Address: _____

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

_____

Signature…….

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): _____

Position: _____

Address: _____

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

_____

Signature…….

(stamp of organisation)

APPENDIX 1

This Appendix forms part of the Clauses and must be completed and signed by the parties
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

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

_____

_____

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

_____

_____

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

_____

_____

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

_____

_____

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

_____

_____

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

_____

_____

DATA EXPORTER	**DATA IMPORTER**
Name: **……..**	Name: **……..**

Authorised signature:	Authorised signature:
……..	……..

APPENDIX 2

This Exhibit must be completed and signed by Data Exporter and Data Importer.

The technical/ organizational security measures implemented by the Data Importer in accordance with Clauses 4(d) and 5(c) (EU Model Clauses) are as set out below:

_____

_____

_____

_____

ILLUSTRATIVE INDEMNIFICATION CLAUSE (OPTIONAL)

Liability

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

(a) the data exporter promptly notifying the data importer of a claim; and

(b) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim[6].

DATA EXPORTER	**DATA IMPORTER**
Name: **……..**	Name: **……..**
Authorised signature:	Authorised signature:
……..	……..

[6] Paragraph on liabilities is optional.