40 28 JANUARY 1981-2021
CONVENTION 108
ON DATA PROTECTION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Strasbourg, 17 November 2023 T-PD(2023)4rev2FINAL

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

CONVENTION 108

Model Contractual Clauses for the Transfer of Personal Data

Module 2:

from Controller to Processor

www.coe.int/dataprotection

Module 2

COUNCIL OF EUROPE
CONVENTION 108+

Model Contractual Clauses for the Transfer of Personal Data from Controller to Processor

Term: Start date [MM/DD/YEAR] – End date [MM/DD/YEAR]]

Data exporter information
Full legal name:
Trading name (if different):
Main address (if a company registered address):
Official registration number (if any):
Key contact (full name, job title, contact details including email):

Data importer information
Full legal name:
Trading name (if different):
Main address (if a company registered address):
Official registration number (if any):
Key contact (full name, job title, contact details including email):

By the signatures of their authorised representatives below, the Data exporter and the Data importer agree to be bound by these Model Contractual Clauses (hereinafter “the Clauses”).

Signed for and on behalf of the Data exporter
Signed:
Date of signature [MM/DD/YEAR]
Full name:
Job title:

Signed for and on behalf of the Data importer
Signed:
Date of signature [MM/DD/YEAR]
Full name:
Job title:

MODEL CONTRACTUAL CLAUSES

PART I – HORIZONTAL CLAUSES

Clause 1. Purpose and scope

1.1. The aim of these Clauses is to ensure compliance with the requirements for the Transfer(s) of Personal data to a Non-Party under Convention 108 as amended by the Protocol CETS No. 223 (hereinafter “the Convention”).

In this regard, these Clauses, together with their Annexes which form an integral part thereof provide an appropriate level of protection for the transfer of Personal data within the meaning of Article 14(2), (3)(b) of the Convention.

1.2. These Clauses shall apply to the Transfer(s) of Personal data as described in Annex 1.

1.2. The purpose(s) of the Transfer(s) of Personal data is described in Annex 1.

Clause 2. Definitions

[Note: Apart from the sources cited with respect to each defined term, see also document T-PD(2020)06rev3, Interpretation of provisions, 7 May 2021. These definitions should be in alphabetical order in the language used.

As used in these Clauses, the following terms starting with a capital letter shall have the following specific meanings:

Applicable law: rules for the protection of Personal data applicable in the jurisdiction of the Data exporter.

Biometric data: data resulting from a specific technical processing of Personal data concerning the physical, biological or physiological characteristics of an individual, which allows the unique identification or authentication of the individual when it is precisely used to uniquely identify the data subject.
[Source: Para. 58 of Explanatory Report].

Convention: Convention for the Protection of Individuals with regard to the processing of Personal Data (ETS No. 108), as amended by Protocol CETS No. 223, adopted by the Committee of Ministers at its 128th Session in Elsinore on 18 May 2018.

Controller: the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has decision-making powers with respect to the Processing.
[Source: Article 2 of the Convention]

Data breach: any accidental or unauthorised access to, destruction, loss, use, modification or disclosure of Personal data due to a violation of the principle of data security.
[Source: Article 7 of the Convention]

Data exporter: the Controller, located in a country that is a Party to the Convention that transfers Personal data to a Data importer.

Data importer: the Processor to which the Data exporter transfers Personal data and that is located in a country that is a Non-Party to the Convention.

Genetic data: all Personal data relating to the genetic characteristics of an individual that have been either inherited or acquired during early prenatal development, as they result from an analysis of a biological sample from the individual concerned including chromosomal, DNA or RNA analysis or analysis of any other element enabling equivalent information to be obtained.
[Source: Para. 57 of the Explanatory Report]

Non-Party: a State that has not ratified the Convention or where it is not yet in force.
[Source: Article 26(3) of the Convention]

Onward transfer: the transfer of Personal data by the Data importer to another Controller or Processor located in the same or in another jurisdiction.

Party (or Parties): the Data importer and/or Data exporter signatories to these Clauses.

Personal data: any information relating to an identified or identifiable individual (hereinafter "Data subject"), whatever his/her nationality or residence.
[Source: Article 2 of the Convention; Para. 15 of the Explanatory Report]

Processing: any operation or set of operations performed on Personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data. Where automated processing is not used, processing means an operation or set of operations performed upon Personal data within a structured set of such data which are accessible or retrievable according to specific criteria.
[Source: Article 2 of the Convention]

Processor: a natural or legal person, public authority, service, agency or any other body that processes Personal data on behalf and under the instructions of the Data exporter.
[Source: Article 2 of the Convention]

Recipient: a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available.
[Source: Article 2 of the Convention]

Special categories of data: (i) genetic data, (ii) Personal data relating to offences, criminal proceedings and convictions, or related security measures; (iii) Biometric data processed for the purpose of uniquely identifying a person; or (iv) Personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life.
[Source: Article 6 of the Convention]

Supervisory authority/ies: one or more authorities responsible for ensuring compliance with the provisions of the Convention as incorporated by the Applicable law.
[Source: Article 15 of the Convention]

Third party beneficiary: the Data subject whose Personal data have been transferred under these Clauses.

Third Party: a natural or legal person, public authority, service, agency or any other body that is not a Party to these Clauses but to which the Personal data is onward transferred by the Data importer, located in the same or in a different jurisdiction as the Data importer.

Transfer: the disclosure or making available of Personal data to a recipient subject to the jurisdiction of a country that is a Non-Party to the Convention.
[Source: Article 14 of the Convention, para. 102 to 104 of the Explanatory report, and the legal opinion provided by the Legal Advisor DLAPIL02/2021_JP/DG3]

Clause 3. Amendment of the Model Contractual Clauses

3.1. These Clauses set out appropriate safeguards, including, obligations for Data exporters and importers, enforceable Data subject rights and effective legal remedies, pursuant to Articles 14(2) and 14(3)(b) of the Convention, provided they are not modified, except to add or update information in the Annexes or to choose an option where it is provided for by the specific Clause.

This does not prevent the Parties from including 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 the Applicable law, or prejudice the human rights and fundamental freedoms of Data subjects recognised in the Convention.

3.2. These Clauses are without prejudice to obligations to which the Data exporter is subject by virtue of the Applicable law.

Clause 4. Interpretation and relation with other agreements

4.1 Where these Clauses use terms that are defined in the Convention, those terms shall have the same meaning as in the Convention, unless they have a specific meaning as set out in Clause 2.

4.2 These Clauses shall be read and interpreted in the light of the provisions of the Convention and its Explanatory Report.

4.3 These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in the Convention as incorporated by the Applicable law. If the meaning of the Clauses is unclear or there is more than one meaning, the meaning which most closely aligns with the Convention applies.

4.4 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. The exception to this is where the conflicting terms of the related agreements provide greater protection for Data subjects, in which case those terms shall prevail over these Clauses.

Clause 5. Execution of the Clauses and Notices

5.1 These Clauses may be executed in any number of counterparts. Once each Party has received a counterpart signed by the other Party (or a digital copy of that signed counterpart), those counterparts will together constitute one and the same instrument and each of which will be, and will be deemed to be, an original.

5.2 Each Party warrants that it has full corporate power and has been duly authorised by all necessary corporate action on its part, to enter into, execute, deliver and perform its obligations under these Clauses.

5.3 All notices and requests under these Clauses by a Party to another Party shall be in writing and shall be served by mail, or by electronic mail to the key contact indicated on the First Page, or to such different addresses as may be communicated by the Party by written notice to the other Party. If the notice or request is sent by e-mail, it will be deemed to have been delivered at the time the e-mail was sent, or if that time is outside of the receiving Party’s normal business hours, the receiving Party’s next normal business day, and provided no notice of non-delivery or bounce back is received.

Clause 6. Accession clause (Optional)

6.1 An entity that is not a Party to these Clauses may, with the agreement of the other Parties, accede to these Clauses at any time, either as a Data exporter or as a Data importer, by completing and signing Annex 2 and, if required, updating the description of the transfer in Annex 1.

6.2 Once it has completed and signed Annex 2, the acceding entity shall become a Party to these Clauses and shall have the rights and obligations of a Data exporter or Data importer in accordance with its designation in Annex 2.

6.3 The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

Clause 7. Third party beneficiaries

The Parties agree and acknowledge that any Data subject whose Personal data were transferred under these Clauses shall be entitled to invoke the safeguards and guarantees set out in Section II and III of these Clauses as a Third-party beneficiary with respect to any provisions of these Clauses affording a right, action, claim, benefit or privilege to such Data subject.

SECTION II – DATA PROTECTION SAFEGUARDS: RIGHTS AND OBLIGATIONS OF THE PARTIES

Clause 8. Instructions

8.1. The Data importer shall process the Personal data only on documented instructions from the Data exporter. The Data exporter may give such instructions throughout the duration of these Clauses.

8.2. The Data importer shall immediately inform the Data exporter if it is unable to follow those instructions.

Clause 9. Purpose limitation

The Data importer shall process the Personal data only for the specific purpose(s) of the Transfer, as set out in Annex 1, unless on further instructions from the Data Exporter.

Clause 10. Transparency of processing

10.1 On request, the Data exporter shall make a copy of these Clauses, including the annexes as completed by the Parties, available to the Data subject free of charge.

10.2 To the extent necessary to protect confidential information, including the measures described in Annex 3 and Personal data, the Data exporter may redact part of the text of the Annex to these Clauses 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.

Clause 11. Accuracy and minimisation of data

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 delay. In this case, the Data importer shall cooperate with the Data exporter to erase or rectify the data without delay.

Clause 12. Duration of processing and erasure or return of data

12.1 Processing by the Data importer shall only take place for the duration specified in Annex 1.

12.2 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 Data exporter 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.

12.3 Until the data is deleted or returned, the Data importer shall continue to ensure compliance with these Clauses.

12.4 In case of domestic laws applicable to the Data importer 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 the data to the extent and for as long as required under that domestic law. The Data exporter should be notified of the relevant domestic law and the required retention period. Only the minimum amount of Personal data should be retained to comply with domestic law.

12.5 This is without prejudice to Clause 22, in particular the requirement for the Data importer under Clause 22 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 22.

Clause 13. Data security

13.1 The Data importer and, during transmission, also the Data exporter shall implement appropriate security measures, both of a technical and organisational nature, for each Processing, in particular to protect against the risk of Data breaches. In adopting such measures, they shall take into account, in particular, the nature of the Processing, the nature and volume of the Personal data processed, the degree of vulnerability of the technical architecture used for the Processing, the state of the art and the cost of implementation. The measures should be commensurate with the seriousness and probability of the potential risks. The Parties shall consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose(s) of Processing can be achieved in that manner.

In the case of pseudonymisation, the additional information for attributing the Personal data to a specific Data subject shall, where possible, remain under the control of the Data exporter.

The Data importer shall grant access to the Personal 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.

13.2 The Parties have agreed on the technical and organisational measures set out in Annex 3. The Data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security and shall update them where this is no longer the case and inform the Data exporter on the result of such checks and relevant changes made in relation thereto.

13.3 If there is a substantial change in the security measures implemented and described in Annex 3, the Parties shall update the Annex.

13.4 In the event of a Data breach concerning Personal data processed by the Data importer under these Clauses, the Data importer shall take appropriate measures to address the Data breach, including measures to mitigate its possible adverse effects.

13.5 The Data importer shall notify – without undue delay and, where feasible, not later than 72 hours after having become aware of the Data breach –the Data exporter, who shall notify the competent Supervisory authority in case the Data breach may seriously interfere with the rights and fundamental freedoms of Data subjects. Data importer will assist the Data exporter in complying with its obligation under its domestic legal framework.

13.6 In both cases, the notification shall include adequate and meaningful information on, notably, the nature of the Data breach, the contact points where more information can be obtained and possible measures that Data subjects could take to address the Data breach, including measures to mitigate its possible adverse effects.

13.7 Where not all the relevant information related to the Data breach is available, notification may take place "in stages", with more information to be provided as soon as it becomes available.

Clause 14. Special categories of data

Where the transfer involves Special categories of data, the Data importer shall apply additional safeguards that guard against and be adapted to the risks that the Processing of such data may present for the interests, rights and fundamental freedoms of the Data subject, notably the risk of discrimination.

Clause 15. Onward transfers

15.1 The Data importer shall only disclose the Personal data to a Third party on documented instructions from the Data exporter.

15.2 In addition, the Data importer shall not onward transfer the Personal data to a Third party unless:

- (a) the law of the third party's jurisdiction, including its international commitments under applicable international treaties or agreements, ensures an appropriate level of protection within the meaning of Article 14 (3)(a) of the Convention, in accordance with the provisions in this regard under Applicable law; or

- (b) the Third party enters into a legally binding and enforceable instrument with the Data importer ensuring the same level of data protection as under these Clauses, and the Data importer provides a copy of these safeguards to the Data exporter; or

- (c) the Onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings in a particular case; or

- (d) the Onward transfer is necessary in a specific case in order to protect the vital interests of the Data subject or of another natural person.

15.3 Any Onward transfer is subject to compliance by the Data importer with all the other safeguards under these Clauses, in particular as regards purpose limitation.

Clause 16. Documentation and compliance

16.1 Each Party must be able to demonstrate compliance with its obligations under these Clauses. To this end, the Data importer shall keep appropriate documentation of the Processing activities carried out on behalf of the Data exporter. The Data importer shall promptly and adequately deal with enquiries from the Data exporter that relate to the Processing under these Clauses.

16.2 The Data importer shall make available to the Data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the Data exporter's request, allow for and contribute to audits of the Processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the Data exporter may take into account relevant certifications held by the Data importer.

16.3 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, which may involve the checking of all physical and digital systems, applications or measures related to data processing and data security including, if it is implied, the use of algorithms or algorithmic processing of the Data importer and shall, where appropriate, be carried out with prior notice.

16.4 The Parties shall make the information referred to in paragraphs 16.2 and 16.3 including the results of any audits, available to the competent Supervisory authority/ies on request.

16.5 The Data importer guarantees that it has carefully considered the impact the intended Processing might have on the rights and fundamental freedoms of Data subjects prior to the commencement of such Processing, according to the circumstances of the specific Transfer, and has taken the necessary and appropriate technical and organisational measures to comply with these Clauses, and to demonstrate such compliance to the competent Supervisory authority/ies. [Source Articles 10(2) and 10(3) of the Convention]

Clause 17. Use of Sub-processors

OPTION 1: SPECIFIC PRIOR AUTHORISATION

17.1 The Data importer shall not sub-contract any of its Processing activities performed on behalf of the Data exporter under these Clauses to a Sub-processor without the Data exporter's prior specific written authorisation. The Data importer shall submit the request for specific authorisation at least [Specify time period]/[leaving enough time for the Data exporter to consider it] prior to the engagement of the sub-processor, together with the information necessary to enable the Data exporter to decide on the authorisation. The list of Sub-processors already authorised by the Data exporter can be found in Annex 4. The Parties shall keep Annex 4 up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION

17.1 The Data importer has the Data exporter's general authorisation for the engagement of Sub-processor(s) from an agreed list. The Data importer shall specifically inform the Data exporter in writing of any intended changes to that list through the addition or replacement of Sub-processors at least [Specify time period] in advance, thereby giving the Data exporter 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 Data exporter with the information necessary to enable the Data exporter to exercise its right to object.

17.2 Where the Data importer engages with the approval of the Data exporter a Sub-processor to carry out specific Processing activities (on behalf of the Data exporter), 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 15. The Data importer shall ensure that the sub-processor complies with the obligations to which the Data importer is subject pursuant to these Clauses.

17.3 The Data importer shall provide, at the Data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the Data exporter. 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.

17.4 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.

17.5 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 transferred.

Clause 18. Rights of Data subjects

18.1 The Data importer shall promptly notify the Data exporter of any request it has received from a Data subject. It shall not respond to that request itself unless it has been instructed to do so by the Data exporter.

18.2 The Data importer shall assist the Data exporter in fulfilling its obligations to respond to Data subjects' requests for the exercise of their rights under these Clauses and the Applicable law. In this regard, the Parties shall set out in Annex 2 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.

18.3 In fulfilling its obligations under paragraphs 18.1 and 18.2, the Data importer shall comply with the instructions from the Data exporter.

Clause 19. Redress for the Data subject

19.1 Where the Data subject invokes a Third-party beneficiary right pursuant to Clause 7, the Data importer shall accept the decision of the Data subject to lodge a complaint with the competent Supervisory authority/ies pursuant to Clause 21, or to refer the dispute to the competent courts pursuant to Clause 26.

19.2 (Optional) The Data importer agrees that Data subjects may lodge a complaint with [INDICATE INDEPENDENT DISPUTE RESOLUTION BODY] at no cost to them. It shall inform the Data subjects in a transparent and easily accessible format, through individual notice or on its website, of such a redress mechanism and that they are not required to use it or follow a particular sequence in seeking redress.

[Note: The Data importer may offer independent dispute resolution through an arbitration body only if such body is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.]

Any possibility to lodge a complaint with an independent dispute resolution body does not exclude or alter the right of the Data subject afforded by these Clauses or the Applicable law to lodge a complaint with the Supervisory Authority/ies or the courts of the competent jurisdiction.

Clause 20. Liability

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

20.2 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 that it causes the Data subject by breaching these Clauses.

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 these Clauses. This is without prejudice to the liability of the Data exporter under the Applicable law.

The Parties agree that if the Data exporter is held liable, under the previous paragraph, 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.

20.3 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.

20.4 The Parties agree that if one Party is held liable under the previous paragraph, it shall be entitled to claim back from the other Party/ies the part of the compensation corresponding to the other Party's/Parties' responsibility for the damage.

20.5 The Data exporter remains responsible for the Processing where it engages a Processor to act on its behalf. The Parties may not invoke the conduct of a sub-Processor to avoid their own liability.
[Source: para. 22 of the Explanatory Report]

Clause 21. Supervisory authority

21.1 The Supervisory authority/ies with responsibility for ensuring compliance by the Data exporter with the Applicable law as regards the Transfer shall act as competent Supervisory authority/ies.

21.2 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, and to abide by its decision. In particular, the Data importer agrees to respond to enquiries, submit to review or 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 – DOMESTIC LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 22. Domestic laws and practices affecting compliance with the Clauses

22.1 The Parties warrant that they have no reason to believe that the laws and practices in the country of destination applicable to the Processing 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 human rights and fundamental freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 11(1) of the Convention, are not in contradiction with these Clauses.

22.2: The Parties declare that in providing the warranty pursuant to previous paragraph, they have taken due account in particular of the following elements:

- (a) the specific circumstances of the Transfer;
- (b) the laws (including case-law) and practices in the country of destination relevant in the specific circumstances of the Transfer;

- (c) any relevant contractual, technical, or organisational safeguards put in place to supplement the safeguards under these Clauses.

22.3 The Data importer warrants that, in carrying out the assessment pursuant to paragraph 22.2, 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.

22.4 The Parties shall document the assessment pursuant to paragraph 22.2 and make it available to the competent Supervisory authority on request.

22.5 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 pursuant to paragraph 22.1, including following a change in the laws of the country of destination 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 22.1.

22.6 Following a notification pursuant to paragraph 22.5, or if the Data exporter otherwise has a 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 Transfer if it considers that no appropriate safeguards for such Transfer can be ensured, or if instructed by 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 24.4 shall apply.

Clause 23. Obligations of the Data importer in case of access by public authorities

23.1 Notification

(a) In so far as domestic law of Data importer allows, the Data importer shall notify the Data exporter, and where possible the Data subjects promptly or use its best efforts to do so - if necessary with the help of the Data exporter -, if it is compelled to preserve, grant access, make available or disclose Personal data transferred from the Data exporter to a Third party including to a public authority.

(b) If the Data importer is prohibited from notifying the Data exporter, then in so far domestic law allows it agrees to use its best efforts to obtain a waiver of the prohibition with a view to communicating as much information as possible. The Data importer agrees to document its efforts in order to be able to demonstrate them to the Data exporter, on request.

(c) Where permissible under the laws of the country of destination, the Data importer agrees to provide the Data exporter, on request, with as much relevant information as possible on any requests for disclosure it has 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.).

(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) Paragraph (a), (b) and (d) is without prejudice to the obligation of the Data importer pursuant to Clause 22.5 and Clause 24 to inform the Data exporter promptly where it is unable to comply with these Clauses.

23.2. Review of legality and data minimisation

(a) The Data importer shall review the legality of any request for disclosure, in particular whether it is 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 and in line with its domestic legislation pursue possibilities of appeal. Pending the determination of any challenge (including on appeal, as relevant) the Data importer shall, to the extent available under domestic legislation, seek interim measures to suspend the effects of the request. These requirements are without prejudice to the obligations of the Data importer under Clause 22.5 and Clause 24.1.

(b) The Data importer shall 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, shall make the relevant documentation available to the Data exporter. It shall also make it available to the competent Supervisory authority on request.

(c) When responding to a request for disclosure, the Data importer shall, having complied with the duty in 23.2, and confirmed the lawfulness of the request provide, only the information which is necessary to respond to the request, in accordance with the domestic legislation.

SECTION IV – FINAL PROVISIONS

Clause 24. Non-compliance with the Clauses and termination

24.1 Each Party shall promptly inform the other Party/ies if it is unable to comply with these Clauses, for whatever reason.

24.2 In the event that the Data exporter has clear information 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 under these Clauses until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 22.6.

24.3 The Data exporter shall be entitled to terminate the contract, insofar as it concerns the Processing of Personal data under these Clauses, where:

(a) the Data exporter has suspended the Transfer of Personal data to the Data importer pursuant to paragraph 24.2 and compliance with the Clauses is not restored within a reasonable time and in any event within one month of suspension;

(b) the Data importer is in substantial or persistent breach of these Clauses; or

(c) the Data importer fails to comply with a binding decision of a competent court or a competent Supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent Supervisory authority 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 non-compliant Party, unless the Parties have agreed otherwise.

24.4 Personal data that has been transferred prior to the termination of the contract pursuant to paragraph 24.3 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 domestic 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 domestic law. The Data exporter should be notified of the relevant domestic law and the required retention period. Only the minimum amount of Personal data should be retained to comply with domestic law.

Clause 25. Governing law

These Clauses shall be governed by the law of the country of the Data exporter.

Alternative in case the law of the country of the Data exporter does not allow for Third party beneficiary rights: These Clauses shall be governed by the law of [INDICATE LAW THAT ENSURES THIRD PARTY BENEFICIARY RIGHTS].

Clause 26. Choice of forum and jurisdiction

26.1 Any dispute arising from these Clauses shall be resolved by the courts of [_____].

26.2 Data subjects may also bring legal proceedings against the Data exporter and/or Data importer before the courts of the country in which they have their habitual residence.

26.3 The Parties agree to submit themselves to the jurisdiction of such courts.

Clause 27. Arbitration

If the Parties are unable to resolve amicably any difference they may have, the dispute shall be finally settled under the Rules of Arbitration (hereinafter, the “Rules”) of the International Chamber of Commerce (“ICC”) by three arbitrators designated by the Parties. Each Party shall designate one arbitrator. The third arbitrator shall be designated by the two arbitrators designated by the Parties. If either Party fails to designate an arbitrator within thirty days after the filing of the dispute with the ICC, such arbitrator shall be appointed in the manner prescribed by the Rules. An arbitration proceeding hereunder shall be conducted in [City, Country], and shall be conducted in [specify language]. The decision or award of the arbitrators shall be in writing and is final and binding on both Parties.

Annex 1
Information about the transfer

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as Data exporter(s) and/or Data importer(s). This does not necessarily require completing and signing separate annexes for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one set of annexes. However, where necessary to ensure sufficient clarity, separate sets of annexes should be used.

Description of the transfer:

- The categories of Data subjects whose data are transferred;
- The categories of Personal data transferred;
- The Special categories of data transferred (where applicable) and the restrictions or safeguards applied, which take full account of the nature of the data and the risks involved, such as, for example, strict purpose limitation, lawful basis for the processing (ex: explicit consent of the Data subject) access restrictions (including access only for staff who have received specific training), restrictions regarding further disclosure, retention of records of data sharing, restrictions on Onward transfers, specific organisational or technical security measures (ex: data encryption, pseudonymisation) or additional security measures;
- The frequency of data transfers (e.g. whether data are transferred once or continuously);
- The nature of the Processing;
- The purpose(s) of the data Transfer and further processing;
- The period for which the Personal data will be stored or, where this is not possible, the criteria for determining this period;

Annex 2
Signature form

[Term: Start date [MM/DD/YEAR] – End date [MM/DD/YEAR]]

Data exporter information
Full legal name:
Trading name (if different):
Main address (if a company registered address):
Official registration number (if any):
Key contact (full name, job title, contact details including email):

Data importer information
Full legal name:
Trading name (if different):
Main address (if a company registered address)::
Official registration number (if any):
Key contact (full name, job title, contact details including email):

By the signatures of their authorised representatives below, the parties agree to be bound by these Model Contractual Clauses (hereinafter “the Clauses”).

Signed for and on behalf of the Data exporter
Signed:
Date of signature [MM/DD/YEAR]
Full name:
Job title:

Signed for and on behalf of the Data importer
Signed:
Date of signature [MM/DD/YEAR]
Full name:
Job title:

Annex 3
Security measures

This annex has to be completed and updated by the Data importer. The technical and organisational measures must be described in specific (and not generic) terms. It must be clearly indicated which measures apply to each transfer/set of transfers.

Examples of possible measures:
Measures of pseudonymisation and encryption of Personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Processing systems and services

Measures for ensuring the ability to restore the availability and access to Personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the Processing

Measures for user identification and authorisation

Measures for the protection of Personal data during transmission

Measures for the protection of Personal data during storage

Measures for ensuring physical security of locations at which Personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure

Annex 4
List of Sub-processors

This annex has to be completed and updated by the Parties with the list of pre-approved Sub-processors according to clause 17.1.