**STANDARD DATA PROTECTION CONTRACTUAL CLAUSES**

**(DIFC Exporter to Non-DIFC Importer in a Third Country with no or**

**unrecognised data protection laws)**

Whereas:

1. The Dubai International Financial Centre (“DIFC”) Standard Data Protection Contractual Clauses (the “DIFC SCCs” or “Clauses”)[[1]](#footnote-1) shall apply to the transfer of Personal Data from a Data Exporter based in the DIFC to Data Importers established in jurisdictions other than the DIFC, whether in UAE or elsewhere (“Third Country”), in accordance with Articles 26 and 27 of the Data Protection Law, DIFC Law No. 5 of 2020 (the “DP Law 2020”) and the Data Protection Regulations 2020 (the “Regulations”), together the Data Protection Legislation (the “DPL”).
2. The DIFC Commissioner of Data Protection (the “Commissioner) may exercise any existing powers to prohibit or suspend data flows to Third Countries in order to protect individuals with regard to the processing of their Personal Data in cases where:
3. it is established that the law in the Third Country to which the Data Importer is subject imposes upon it requirements to deviate from the DPL that results in a substantial adverse effect on the guarantees provided by the DPL;
4. another relevant supervisory authority has established that the Data Importer has not respected the DPL or comparable data protection laws and regulations or the standard contractual clauses in the Annex; or
5. there is a substantial risk that the Data Processing Clauses in the Annex are not being or will not be complied with and the continuing transfer would result in imminent, grave harm to Data Subjects whose Personal Data is being processed.
6. If such prohibitive or limiting measures are adopted, interested parties should be informed without delay.
7. The prohibitive or limiting measures set out above shall be lifted when the Commissioner is satisfied that the reasons for the suspension or prohibition no longer exist.
8. Defined terms have the same meeting as set out in Schedule 1, Article 3 of the DP Law 2020.
9. [This DPA shall be effective from the date stated above. The term of this DPA shall be three (3) years, at which time it will be reviewed and updated as needed in order to comply with then-current applicable data protection laws.][[2]](#footnote-2)
10. The Parties agree the following SCCs for the transfer of Personal Data to a Data Importer located in a jurisdiction without a data protection law equivalent or substantially encompassing the principles set out in the DPL:

ANNEX

**Clause 1: Purpose and Scope**

1. Purpose and Scope
2. The purpose of these Clauses is to ensure compliance with the requirements of the DPL for the protection of individuals with regard to the processing, including transfers, of Personal Data.
3. The Parties:
4. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the Personal Data out of the DIFC, as listed in Appendix 1 (the “Data Exporter”); and
5. the entity/ies in a Third Country receiving the Personal Data from the Data Exporter, directly or indirectly via an another intermediary entity also Party to these Clauses, as listed in Appendix 1 (the “Data Importer”)

have agreed to these Clauses in accordance with Article 27(2)(c) of the DPL.

1. These Clauses apply with respect to the transfer of Personal Data as specified in Appendix 1.
2. The Appendices to these Clauses form an integral part of these Clauses.

**Clause 2: Effect and invariability of the Clauses**

For the purposes of compliance with the DPL, the Parties have agreed that the clauses delineated below (the “Data Processing Clauses” or the “Clauses”) offer adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights as required by the DPL, and for Onward Transfers (if any) of Personal Data under Articles 26, 27, and 32 to 40 of the DPL, provided they are not modified except to add or update information in the Appendices or to adopt equivalent, approved Clauses. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of Data Subjects.

**Clause 3: Third Party beneficiaries**

1. The Parties agree that a Data Subject may as a Third Party beneficiary enforce this Clause and any relevant Clauses under which rights inure to the Data Subject’s benefit against the Data Importer or the Data Exporter, for their respective breach of their contractual obligations herein, with regard to his Personal Data, and accept jurisdiction for this purpose.
2. The Parties agree that clause 3(1) will apply 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 any other parties to these Clauses under which rights inure to the Data Subject’s benefit, in cases where both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the Data Exporter, in which case the Data Subject can enforce them against such entity. Such Third Party liability shall be limited to its own processing operations under these 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 Applicable Law.
5. Clauses (1) to (4) are without prejudice to rights of Data Subjects under the DPL or Regulations.

**Clause 4: Interpretation**

1. Where these Clauses use the terms that are defined in the DPL Schedule 1, Article 3, those terms shall have the same meaning as found therein.
2. These Clauses shall be read and interpreted in the light of the provisions of the DPL or Regulations.
3. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in the DPL or Regulations.

**Clause 5: Hierarchy**

1. 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, even if those agreements have been negotiated by the Parties.
2. The exceptions to this are where (and in so far as):
3. the inconsistent or conflicting terms of the related agreement provide greater protection for the Data Subject’s rights, in which case those terms will override these Clauses; or
4. the inconsistent or conflicting terms of the related agreement are expressly required by and validly drafted in accordance with Article 24 of the DP Law 2020, in which case those terms will override these Clauses.

**Clause 6: Description of the Transfers**

The details of the transfer(s), and in particular the categories of Personal Data that are transferred and the purpose(s) for which they are transferred, are specified in Appendix 1.

**Clause 7: Docking Clause [Optional]**

1. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a Data Exporter or as a Data Importer, by completing and signing the relevant Appendices.
2. Once it has completed and signed the relevant Appendices, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a Data Exporter or Data Importer in accordance with its designation in Appendix 1.
3. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

**OBLIGATIONS OF THE PARTIES**

**Clause 8: Data Protection Safeguards**

1. The Data Exporter warrants that it has used reasonable efforts to determine that the Data Importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.
2. Controllers (including Joint or Co-Controllers) may share data for a common purpose or for independent purposes, in accordance with Article 23 of the DP Law 2020.
3. Where, in accordance with these Clauses, Personal Data is disclosed to or by Processors or Sub-processors only, the following obligations shall apply:
4. Where the Parties to these Clauses are Processors or Sub-processors only, each Party is required to act under the instructions of the relevant Controller(s) with which they have legally binding written agreements in accordance with Articles 23 and / or 24 of the DP Law 2020, and which shall be made available prior to Processing.
5. Any additional instructions set out in legally binding written agreements between them that were not provided by the Controller shall not conflict with the Controller’s instructions hereto. Further documented instructions regarding the Processing may be subsequently agreed at any time.
6. Any Party shall immediately inform all other Parties if it is unable to follow those instructions.
7. The Parties warrant that all legally binding agreements or other legal act under DIFC law ensure full delegation of the obligations that any Processor or Sub-processor owes to the Controller under the agreement with the Controller in respect of such specific Processing activities, in accordance with Article 24(3).
8. After the end of the provision of the Processing services, if requested by a Party where reasonable to do so and subject to any reasonable objections, the Processors or Sub-processors shall delete all Personal Data processed and certify to the Parties that it has done so, or return to the Controller all Personal Data processed on its behalf and delete existing copies. If any Party objects to such request, it shall be reviewed and any agreed actions must be documented in writing.
9. In all data sharing arrangements, the Data Exporter and Data Importer shall implement the data protection safeguards, as set out in sub-sections A to I below:
10. **Purpose Limitation**
11. The Data Importer shall process the Personal Data only for the specific purpose(s) of the transfer, as set out in Appendix 1 or if otherwise agreed through formal instructions.
12. Where the Data Importer is a Controller, it may only do so for another purpose:
13. where it has obtained the Data Subject’s prior consent;
14. where necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
15. where necessary in order to protect the vital interests of the Data Subject or of another natural person.
16. **Transparency**
17. In order to enable Data Subjects to effectively exercise their rights pursuant to the DPL or these Clauses, they shall be informed by the Data Importer or directly or through the Data Exporter, as appropriate, of:
18. the identity and contact details of the Disclosing Party;
19. the categories of Personal Data processed;
20. the right to obtain a copy of these Clauses;
21. where any Party intends to Onward Transfer the Personal Data to any Third Party/ies, the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such Onward Transfer, and the ground(s) therefore pursuant to clause 8(G).
22. Clause 8(B)(i) shall not apply where the Data Subject already has the information, including when such information has already been provided by the Data Exporter, or providing the information proves impossible or would involve a disproportionate effort for the Data Importer. In the latter case, the Data Importer shall, to the extent possible, make the information publicly available.
23. On request, the Parties shall make a copy of these Clauses, including the Appendices as completed by them, available to the Data Subject free of charge. To the extent necessary to protect business secrets or other confidential information, including Personal Data of others, the Parties may redact part of the text of an Appendix prior to sharing a copy, but shall provide a meaningful summary where the Data Subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the Data Subject with the reasons for the redactions, to the extent possible without revealing the redacted information.
24. Clauses 8B(i) to (3) are without prejudice to the obligations of the Data Exporter under Articles 29 and 30 of DPL.
25. **Accuracy and Minimisation**
26. Personal Data must be accurate and, where necessary, kept up to date. Every reasonable step shall be taken by all Parties to ensure that Personal Data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.
27. If one of the Parties becomes aware that the Personal Data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.
28. Wherever applicable, the Parties shall ensure that the Personal Data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.
29. **Storage limitation / Duration of processing and erasure or return of data**
30. Processing by the Data Importer shall only take place for the duration specified in Appendix 1.
31. The Data Importer shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation[[3]](#footnote-3) of the data and all back-ups at the end of the retention period.
32. After the processing for the relevant purposes ends, 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.
33. Until the data is deleted or returned, the Data Importer shall continue to ensure compliance with these Clauses. In case of applicable local laws that prohibit return or deletion of the Personal Data, the Parties warrant that they will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law.
34. The above obligations are without prejudice to clause 14, in particular the requirement for the Data Importer under clause 14(5) 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 14(1).
35. **Security of Processing**
36. The Data Importer and, during transmission, also the Data Exporter shall implement appropriate technical and organisational measures to ensure the security of the Personal Data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter ‘Personal Data Breach’). In assessing the appropriate level of security, they shall take due account of the then-current emerging or advanced technology, the costs of implementation, the nature of the Personal Data[[4]](#footnote-4), the scope, context and purpose(s) of processing and the risks involved in the processing for the Data Subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the Personal Data to a specific Data Subject shall, where possible, remain under the exclusive control of the Data Exporter.
37. The Parties have agreed on the technical and organisational measures set out in Appendix 2. The Data Importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
38. 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.
39. In the event of a Personal Data Breach concerning Personal Data processed by the Data Importer under these Clauses, the Data Importer shall take appropriate measures to address the Personal Data Breach, including measures to mitigate its possible adverse effects.
40. In case of a Personal Data Breach that is likely to result in a risk to the rights and freedoms of natural persons, the Data Importer shall without undue delay notify both the Data Exporter and the competent supervisory authority pursuant to clause 13. Such notification shall contain:
41. a description of the nature of the breach (including, where possible, categories and approximate number of Data Subjects and Personal Data records concerned),
42. its likely consequences,
43. the measures taken or proposed to address the breach, and
44. the details of a contact point from whom more information can be obtained. To the extent it is not possible for the Data Importer to provide all the information at the same time, it may do so in phases without undue further delay.
45. In case of a Personal Data Breach that is likely to result in a high risk to the rights and freedoms of natural persons, the Data Importer shall also notify without undue delay the Data Subjects concerned of the Personal Data Breach and its nature, if necessary in cooperation with the Data Exporter, together with the information referred to in clause 8(E)(v), points (b) to (d), unless the Data Importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the Data Importer shall instead issue a public communication or take a similar measure to inform the public of the Personal Data Breach.
46. The Data Importer shall document all relevant facts relating to the Personal Data Breach, including its effects and any remedial action taken, and keep a record thereof. The Data Importer shall also include in such record the steps it takes to prevent the Personal Data Breach from happening again and to ensure that the data protection safeguards continue to provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Data Subjects of such a Personal Data Breach.
47. **Special Category Data**
48. Where the transfer involves Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter ‘sensitive data’), the Data Importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved, as described in Appendix 2.
49. This may include restricting the personnel permitted to access the Personal Data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.
50. **Onward Transfers**
51. The Data Importer shall not disclose the Personal Data to a Third Party in the same country as the Data Importer or in another Third Country, (hereinafter ‘Onward Transfer’) unless the Third Party is or agrees to be bound by these Clauses. Otherwise, an Onward Transfer by the Data Importer may only take place if:
52. it is to a country benefitting from an adequacy decision pursuant to Article 26 of the DPL that covers the Onward Transfer;
53. the Third Party otherwise ensures appropriate safeguards pursuant to Articles 26 and 27 of the DPL with respect to the processing in question;
54. the Third Party enters into a binding 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;
55. it is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings;
56. it is necessary in order to protect the vital interests of the Data Subject or of another natural person; or
57. where none of the other conditions apply, the Data Importer has obtained the explicit consent of the Data Subject for an Onward Transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the Data Importer shall inform the Data Exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the Data Subject.
58. Any Onward Transfer is subject to compliance by the Data Importer with all the other safeguards under these Clauses, in particular purpose limitation, as well as any valid instructions from the Controller, where applicable.
59. **Processing under the authority of the Data Importer**

The Data Importer shall ensure that any person acting under its authority processes the data only on its instructions.

1. **Documentation and Compliance**
2. The Data Importer shall promptly and adequately deal with enquiries from the Data Exporter that relate to the processing under these Clauses.
3. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the Data Importer shall keep appropriate documentation on the processing activities carried out on behalf of the Controller.
4. Where required, the Data Importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the Data Exporter.
5. The Data Importer shall allow for and contribute to audits by the Data Exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the Data Exporter requests an audit on instructions of a Controller.
6. Where an audit is carried out on the instructions of the Controller, the Data Exporter shall make the results available to the Controller.
7. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the Data Importer and shall, where appropriate, be carried out with reasonable notice.
8. In any case, the data exporter may take into account relevant certifications held by the Data Importer.
9. The Parties shall make the information referred to in this Clause 8(I), including the results of any audits, available to the competent supervisory authority on request.

**Clause 9: Use of Sub-processors**

1. Where the Data Exporter is a Controller and the Data Importer is a Processor, the following is required:
2. [FOR THIS SUB-PARAGRAPH, PLEASE CHOOSE OPTION 1 or 2]

**OPTION 1: SPECIFIC PRIOR AUTHORISATION** 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] 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 Appendix 3. The Parties shall keep Appendix 3 up to date.

**OPTION 2: GENERAL WRITTEN AUTHORISATION** 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.

1. Where the Data Importer engages 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[[5]](#footnote-5). The Parties agree that, by complying with this Clause, the Data Importer fulfils its obligations under clauses 8(H) and 8(I). The Data Importer shall ensure that the Sub-processor complies with the obligations to which the Data Importer is subject pursuant to these Clauses and must ensure that any person or third party acting under its authority, including a Sub-processor, only Process the Personal Data on its instructions.
2. 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.
3. 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.
4. 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.
5. Where the Data Exporter is a Processor Processing Personal Data on behalf of a Controller, and the Data Importer is also a Processor (or Sub-processor), the following is required:
6. [FOR THIS SUB-PARAGRAPH, PLEASE CHOOSE OPTION 1 or 2]

**OPTION 1: SPECIFIC PRIOR AUTHORISATION** 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 prior specific written authorisation of the Controller. The Data Importer shall submit the request for specific authorisation at least [Specify time period] prior to the engagement of the Sub-processor, together with the information necessary to enable the Controller to decide on the authorisation. It shall inform the Data Exporter of such engagement. The list of Sub-processors already authorised by the Controller can be found in Appendix 3. The Parties shall keep Appendix 3 up to date.

**OPTION 2: GENERAL WRITTEN AUTHORISATION** The Data Importer has the Controller’s general authorisation for the engagement of Sub-processor(s) from an agreed list. The Data Importer shall specifically inform the Controller in writing of any intended changes to that list through the addition or replacement of Sub-processors at least [Specify time period] in advance, thereby giving the Controller sufficient time to be able to object to such changes prior to the engagement of the Sub-processor(s). The Data Importer shall provide the Controller with the information necessary to enable the Controller to exercise its right to object. The Data Importer shall inform the Data Exporter of the engagement of the Sub-processor(s).

1. Where the Data Importer engages a Sub-processor to carry out specific processing activities (on behalf of the Controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the Data Importer under these Clauses, including in terms of Third Party beneficiary rights for Data Subjects[[6]](#footnote-6). The Parties agree that, by complying with this Clause, the Data Importer fulfils its obligations under clause 8(H). The Data Importer shall ensure that the Sub-processor complies with the obligations to which the Data Importer is subject pursuant to these Clauses and must ensure that any person or third party acting under its authority, including a Sub-processor, only Process the Personal Data on its instructions.
2. The Data Importer shall provide, at the Data Exporter’s or Controller’s request, a copy of such a Sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including Personal Data, the Data Importer may redact the text of the agreement prior to sharing a copy.
3. 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.
4. The Data Importer shall agree a Third Party beneficiary clause with the Sub-processor whereby – in the event the Data Importer has factually disappeared, ceased to exist in law or has become insolvent – the Data Exporter shall have the right to terminate the Sub-processor contract and to instruct the Sub-processor to erase or return the Personal Data.

**Clause 10: Data Subjects’ Rights**

1. Where the Data Importer is another Controller:
2. The Data Importer, where relevant with the assistance of the Data Exporter, shall deal with any enquiries and requests it receives from a Data Subject relating to the processing of his/her Personal Data and the exercise of his/her rights under these Clauses and under the local law applicable to the Data Importer, without undue delay and at the latest within one month of the receipt of the enquiry or request[[7]](#footnote-7). The Data Importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of Data Subject rights. Any information provided to the Data Subject shall be in an intelligible and easily accessible form, using clear and plain language.
3. In particular, upon request by the Data Subject the Data Importer shall, free of charge:
4. provide confirmation to the Data Subject as to whether Personal Data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Appendix 1; if Personal Data has been or will be Onward Transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the Personal Data has been or will be Onward Transferred, the purpose of such Onward Transfers and their ground pursuant to clause 8(G); and provide information on the rights to lodge a complaint with a supervisory authority and to bring a claim for compensation under these Clauses;
5. rectify inaccurate or incomplete data concerning the Data Subject; and
6. erase Personal Data concerning the Data Subject if such data is being or has been processed in violation of any of these Clauses ensuring Third Party beneficiary rights, or if the Data Subject withdraws the consent on which the processing is based.
7. Where the Data Importer processes the Personal Data for direct marketing purposes, it shall cease processing for such purposes if the Data Subject objects to it.
8. The Data Importer shall not make a decision based solely on the automated processing of the Personal Data transferred (hereinafter ‘automated decision’), which would produce legal effects concerning the Data Subject or similarly significantly affect him/her, unless with the explicit consent of the Data Subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the Data Subject’s rights and legitimate interests. In this case, the Data Importer shall, where necessary in cooperation with the Data Exporter:
9. inform the Data Subject about the envisaged automated decision, the envisaged consequences and the logic involved; and
10. implement suitable safeguards, at least by enabling the Data Subject to contest the decision, express his/her point of view and obtain review by a human being.
11. Where requests from a Data Subject are excessive, in particular because of their repetitive character, the Data Importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.
12. The Data Importer may refuse a Data Subject’s request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in the DPL.
13. If the Data Importer intends to refuse a Data Subject’s request or charge a reasonable fee, it shall inform the Data Subject of the reasons for the refusal of the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress and that the Data Subject is entitled to bring a claim for compensation under these Clauses.
14. Where the Data Importer is another Processor (or Sub-processor):
15. 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 authorised to do so by the Data Exporter.
16. 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 the DPL and under the local law, if any, applicable to the Data Importer. In this regard, the Parties shall set out in Appendix 2 the appropriate technical and organisational measures, taking into account the nature of the processing, the means by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
17. In fulfilling its obligations under clauses 10(2)(a) and (b), the Data Importer shall comply with the instructions from the Data Exporter.

**Clause 11: Redress**

1. The Data Importer shall inform Data Subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a Data Subject. The Data Importer agrees that Data Subjects may also lodge a complaint with an independent dispute resolution body[[8]](#footnote-8) at no cost to the Data Subject. It shall inform the Data Subjects, in the manner set out above, of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.
2. In case of a dispute between a Data Subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
3. Where the Data Subject invokes a Third Party beneficiary right pursuant to clause 3, the Data Importer shall accept the decision of the Data Subject to:
4. lodge a complaint with the Commissioner or other supervisory authority in his/her habitual residence or place of work (where applicable), or the competent supervisory authority pursuant to clause 13; or
5. refer the dispute to the competent courts within the meaning of clause 18.
6. The Data Importer shall abide by a decision that is binding under the DPL or other applicable laws.
7. The Data Importer agrees that the choice made by the Data Subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

**Clause 12: Liability**

1. Where the Data Importer is a Controller
2. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
3. Each Party 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 the Party causes the Data Subject by breaching the Third Party beneficiary rights under these Clauses. This is without prejudice to any other liability of the Data Exporter under the DPL.
4. 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.
5. The Parties agree that if one Party is held liable under clause 12(1)(c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
6. The Data Importer may not invoke the conduct of a Processor or Sub-processor to avoid its own liability.
7. Where the Data Importer is a Processor:
8. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
9. The Data Importer shall be liable to the Data Subject, and the Data Subject shall be entitled to receive compensation, for any material or non-material damages the Data Importer or its Sub-processor causes the Data Subject by breaching the Third Party beneficiary rights under these Clauses.
10. Notwithstanding clause 12(2)(b), the Data Exporter shall be liable to the Data Subject, and the Data Subject shall be entitled to receive compensation, for any material or non-material damages the Data Exporter or the Data Importer (or its Sub-processor) causes the Data Subject by breaching the Third Party beneficiary rights under these Clauses. This is without prejudice to the liability of the Data Exporter and, where the Data Exporter is a Processor acting on behalf of a Controller, to the liability of the Controller under the DPL or other applicable laws.
11. The Parties agree that if the Data Exporter is held liable under clause 12(2)(c) for damages caused by the Data Importer (or its Sub-processor), it shall be entitled to claim back from the Data Importer that part of the compensation corresponding to the Data Importer’s responsibility for the damage.
12. 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.
13. The Parties agree that if one Party is held liable under clause 12(2)(e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
14. The Data Importer may not invoke the conduct of a Sub-processor to avoid its own liability.

**Clause 13: Supervision**

1. The supervisory authority with responsibility for ensuring compliance by the Data Exporter with the DPL as regards the data transfer(s), as indicated in Appendix 1, is the Commissioner.
2. The Data Importer agrees, for the purposes and context of such Processing, to submit itself to the jurisdiction of and cooperate with the Commissioner in any procedures aimed at ensuring compliance with these Clauses. In particular, the Data Importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the Commissioner with written confirmation that the necessary actions have been taken.

**Clause 14: Local Laws and Practices Affecting Compliance with the Clauses**

1. The Parties warrant that they have no reason to believe that the laws and practices in the Third Country of destination applicable to the processing of the Personal Data by the Data Importer, including any requirements to disclose Personal Data or measures authorising access by public authorities, prevent the Data Importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate to safeguard the objectives listed in the DPL, are not in contradiction with these Clauses.
2. The Parties declare that in providing the warranty in clause 14(1), they have taken due account in particular of the following elements:
3. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended Onward Transfers; the type of recipient; the purpose of processing; the categories and format of the transferred Personal Data; the economic sector in which the transfer occurs; the storage location of the data transferred;
4. the laws and practices of the Third Country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[[9]](#footnote-9);
5. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the Personal Data in the country of destination; or
6. an assessment of the importing jurisdiction made in accordance with guidance and any associated tools or indexes provided by the Commissioner.
7. The Data Importer warrants that, in carrying out the assessment under clause 14(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.
8. The Parties agree to document the assessment under clause 14(2) and make it available to the competent supervisory authority on request.
9. The Data Importer agrees to notify the Data Exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under clause 14(1), including following a change in the laws of the Third Country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in clause 14(1). Where necessary, the Data Exporter shall forward the notification to the Controller.
10. Following a notification pursuant to clause 14(5), or if the Data Exporter otherwise has reason to believe that the Data Importer can no longer fulfil its obligations under these Clauses, the Data Exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the Data Exporter and/or Data Importer to address the situation, if appropriate in consultation with the Controller. The Data Exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the Controller (where appropriate) or the competent supervisory authority to do so. In this case, the Data Exporter shall be entitled to terminate the contract, insofar as it concerns the processing of Personal Data under these Clauses. If the contract involves more than two Parties, the Data Exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, clauses 16(4) and (5) shall apply.

**Clause 15: Notification**

Notification

1. The Data Importer agrees to notify the Data Exporter and, where possible, the Data Subject promptly (if necessary with the help of the Data Exporter) if it:
2. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of Personal Data transferred pursuant to these Clauses; such notification shall include information about the Personal Data requested, the requesting authority, the legal basis for the request and the response provided; or
3. becomes aware of any direct access by public authorities to Personal Data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer. Where necessary the Data Exporter shall forward the notification to the Controller.
4. If the Data Importer is prohibited from notifying the Data Exporter and/or the Data Subject under the laws of the country of destination, the Data Importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The Data Importer agrees to document its best efforts in order to be able to demonstrate them on request of the Data Exporter.
5. Where permissible under the laws of the country of destination, the Data Importer agrees to provide the Data Exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). Where necessary, the Data Exporter shall forward the information to the Controller.
6. The Data Importer agrees to preserve the information pursuant to clauses 15(1) to (3) for the duration of the contract and make it available to the competent supervisory authority on request.
7. Clauses 15(1) to (3) are without prejudice to the obligation of the Data Importer pursuant to clause 14(5) and clause 16 to inform the Data Exporter promptly where it is unable to comply with these Clauses.

Review of legality and data minimisation

1. The Data Importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The Data Importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the Data Importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the Personal Data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the Data Importer under clause 14(5).
2. The Data Importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the Data Exporter. It shall also make it available to the competent supervisory authority on request. Where necessary, the Data Exporter shall make any related assessment available to the Controller or Data Importer.
3. The Data Importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

**Clause 16: Non-compliance with the Clauses and termination**

1. The Data Importer shall promptly inform the Data Exporter if it is unable to comply with these Clauses, for whatever reason.
2. In the event that the Data Importer is in breach of these Clauses or unable to comply with these Clauses, the Data Exporter shall suspend the transfer of Personal Data to the Data Importer until compliance is again ensured or the contract is terminated. This is without prejudice to clause 14(6).
3. The Data Exporter shall be entitled to terminate the contract, insofar as it concerns the processing of Personal Data under these Clauses, where:
4. the Data Exporter has suspended the transfer of Personal Data to the Data Importer pursuant to clause 16(2) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
5. the Data Importer is in substantial or persistent breach of these Clauses; or
6. the Data Importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority if necessary[[10]](#footnote-10), and the Controller of such non-compliance. Where the contract involves more than two Parties, the Data Exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

1. Personal Data that has been transferred prior to the termination of the contract pursuant to clause 16(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. Personal Data collected by the Data Exporter that has been transferred prior to the termination of the contract pursuant to clause 16(3) shall immediately be deleted by the importer in its entirety, including any copy thereof[[11]](#footnote-11). The Data Importer shall certify the deletion of the data to the Data Exporter. Until the data is deleted or returned, the Data Importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the Data Importer that prohibit the return or deletion of the transferred Personal Data, the Data Importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
2. Either Party may revoke its agreement to be bound by these Clauses where the Commissioner adopts a decision pursuant to Article 26 of DPL that covers the transfer of Personal Data to which these Clauses apply. This is without prejudice to other obligations applying to the processing subject to the DPL.
3. [OPTIONAL: Where circumstances of the transfers covered by these Clauses change, including where they are no longer required, the Parties may terminate this DPA by providing [sixty (60)] days written notice to the other.]

**Clause 17: Governing Law**

These Clauses shall be governed by the laws and regulations of the DIFC.

**Clause 18: Jurisdiction**

Any dispute arising from these Clauses shall be resolved by the Courts of the DIFC. A Data Subject may also bring legal proceedings against a Party before the courts of the jurisdiction in which he/she has his/her habitual residence, provided a comparable data protection regime exists in such jurisdiction. The Parties agree to submit themselves to the jurisdiction of such courts.

**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(s):**

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 to the DATA PROCESSING Clauses

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

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

**Data Exporter**

Name: …

Address: …

Contact person’s name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (Controller/Processor): …

The Data Exporter (please specify briefly your activities relevant to the transfer):

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**Data Importer**

The Data Importer (please specify briefly activities relevant to the transfer):

Name: …

Address: …

Contact person’s name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (Controller/Processor): …

…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………..

**Data Subjects**

The Personal Data transferred concerns the following categories of Data Subjects (please specify):

……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**Categories of data**

The Personal Data transferred concerns the following categories (please specify):

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**Special categories of data (if any)**

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

The Personal Data transferred concern the following Special categories of data (please specify):

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**Processing operations**

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

Please describe the frequency of the transfer(s)

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

***Nature*** *of the processing*

The Personal Data transferred will be subject to the following basic processing activities (please specify):

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

***Purpose(s)*** *of the data transfer and further processing*

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

***Retention period*** *for which the Personal Data will be processed, if any, and the criteria used to determine that period*

……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

*For transfers to* ***(Sub-) Processors****, also specify* ***subject matter, nature and duration*** *of such further processing*

……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

*Identify whether* ***any other competent supervisory authority/ies*** *may have jurisdiction in accordance with clause 13*

……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**DATA EXPORTER**

Name:………………………………

Signature ……………………

**DATA IMPORTER**

Name:………………………………

Signature:……………………

Appendix 2 to the DATA PROCESSING Clauses

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

**Description of the technical and organisational security measures implemented by the Data Importer in accordance with these Clauses (or document/legislation attached):**

*Description of the technical and organisational measures implemented by the Data Importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.*

***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 data during transmission*
* *Measures for the protection of 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*

*For transfers to* ***(Sub-)Processors****, also* *describe the* ***specific technical and organisational measures to be taken by the (Sub-)Processor*** *to be able to provide assistance to the Controller and, for transfers from a Processor to a Sub-processor, to the Data Exporter*

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………..

Appendix 3: List of Sub-processors

Where applicable, the Controller has authorised the use of the following Sub-processors:

|  |  |  |
| --- | --- | --- |
|  | 1. | Name: …  Address: …  Contact person’s name, position and contact details: …  Description of processing (including a clear delimitation of responsibilities in case several Sub-processors are authorised): … |

|  |  |  |
| --- | --- | --- |
|  | 2.Repeat as needed, or insert table based on this [Record of Processing Activities template](https://www.difc.ae/application/files/6416/2021/0422/SAMPLE_DIFC_ROPA.xlsx) | … |

1. Replace with the words ‘This Data Protection Agreement (“DPA”)’ throughout, when used as a standalone agreement. [↑](#footnote-ref-1)
2. This clause applies and should be included when used as a standalone DPA. [↑](#footnote-ref-2)
3. This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with prevailing guidance and technology in this regard, and that this process is irreversible. [↑](#footnote-ref-3)
4. This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions or offences [↑](#footnote-ref-4)
5. This requirement may be satisfied by the Sub-processor acceding to these Clauses in accordance with clause 7. [↑](#footnote-ref-5)
6. This requirement may be satisfied by the Sub-processor acceding to these Clauses in accordance with clause 7. [↑](#footnote-ref-6)
7. That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The Data Importer shall duly and promptly inform the Data Subject of any such extension [↑](#footnote-ref-7)
8. The Data Importer may offer independent dispute resolution through an arbitration body only if it agrees to be subject to the Arbitration Law, DIFC Law No 1 of 2008 and DIFC Arbitration Rules, or is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards [↑](#footnote-ref-8)
9. As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the Data Importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies. [↑](#footnote-ref-9)
10. For example, where the Data Importer is a Processor or Sub-processor [↑](#footnote-ref-10)
11. For example, where the Data Importer is a Controller [↑](#footnote-ref-11)