

Schedule 1

CONTROLLER-TO-CONTROLLER STANDARD CONTRACTUAL CLAUSES

relating to the transfer of Personal Data outside the ADGM pursuant to the Abu Dhabi Global Market Data Protection Regulations 2021

SECTION I

Clause 1

Purpose and scope

- 1.1 The purpose of these standard contractual clauses is to ensure compliance with the requirements of the Abu Dhabi Global Market (“**ADGM**”) Data Protection Regulations 2021 (“**DPR 2021**”) relating to the transfer of Personal Data outside the ADGM.
- 1.2 The parties:
 - (a) the natural or legal persons, public authorities, agencies or other bodies transferring the Personal Data, as listed in ANNEX I.A. (the “**data exporter**”), and
 - (b) the entities in a jurisdiction outside of the ADGM receiving the Personal Data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in ANNEX I.A (the “**data importer**”),((a) and (b) together the “**Parties**”),
have agreed to these standard contractual clauses (the “**Clauses**”).
- 1.3 These Clauses apply with respect to the transfer of Personal Data as specified in ANNEX I.B.
- 1.4 The Appendix to these Clauses containing the Annexes forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

- 2.1 These Clauses set out appropriate safeguards, including enforceable Data Subject rights and effective legal remedies, pursuant to section 42(1) and section 42(2) of the DPR 2021 and, with respect to data transfers from Controllers to Processors and Processors to Processors, standard contractual clauses pursuant to section 26(6) of the DPR 2021, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses 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.

- 2.2 These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of the DPR 2021.

Clause 3

Third-party beneficiaries

- 3.1 Data Subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and data importer, with the following exceptions:
- (a) Clause 1, Clause 2, Clause 3, Clause 6, 오류! 참조 원본을 찾을 수 없습니다.;
 - (b) Clause 7 - Module One: Clause 7.5(e) and Clause 7.5(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
 - (c) Clause 8 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
 - (d) Clause 11 - Module One: Clause 11(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
 - (e) Clause 12;
 - (f) Clause 14.1(c), (d) and (e);
 - (g) Clause 15(e);
 - (h) Clause 17.
- 3.2 Paragraph 3.1 is without prejudice to rights of Data Subjects under the DPR 2021.

Clause 4

Interpretation

- 4.1 Where these Clauses use terms that are defined in the DPR 2021, those terms shall have the same meaning as in the DPR 2021.
- 4.2 These Clauses shall be read and interpreted in the light of the provisions of the DPR 2021.
- 4.3 These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in the DPR 2021.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 7

Data protection safeguards

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

7.1 Purpose limitation

The data importer will Process the Personal Data only for the specific purpose(s) of the transfer, as set out in ANNEX I.B. It may only Process the Personal Data for another purpose:

- (a) where it has obtained the Data Subject's prior consent;
- (b) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (c) where necessary in order to protect the vital interests of the Data Subject or of another natural person.

7.2 Transparency

- (a) In order to enable Data Subjects to effectively exercise their rights pursuant to Clause 9, the data importer will inform them, either directly or through the data exporter:
 - (i) of its identity and contact details;
 - (ii) of the categories of Personal Data Processed;
 - (iii) of the right to obtain a copy of these Clauses; and
 - (iv) where it intends to onward transfer the Personal Data to any third party/ies, of the Recipient or categories of Recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

- (b) Paragraph (a) will 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 will, to the extent possible, make the information publicly available.
- (c) On request, the Parties will make a copy of these Clauses, including the Appendix 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, the Parties may redact part of the text of the Appendix prior to sharing a copy, but will provide a meaningful summary where the Data Subject would otherwise not be able to understand its content or exercise his or her rights. On request, the Parties will provide the Data Subject with the reasons for the redactions, to the extent possible without revealing the redacted information.
- (d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under sections 11 and 12 of the DPR 2021.

7.3 Accuracy and data minimisation

- (a) Each Party will ensure that the Personal Data is accurate and, where necessary, kept up to date. The data importer will take every reasonable step to ensure that Personal Data that is inaccurate, having regard to the purpose(s) of Processing, is erased or rectified without delay.
- (b) If one of the Parties becomes aware that the Personal Data it has transferred or received is inaccurate, or has become outdated, it will inform the other Party without undue delay.
- (c) The data importer will ensure that the Personal Data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of Processing.

7.4 Storage limitation

The data importer will retain the Personal Data for no longer than necessary for the purpose(s) for which it is Processed. It will put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

7.5 Security of Processing

- (a) The data importer and, during transmission, also the data exporter will 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 will take due account of the State Of The Art, the costs of implementation, the nature, scope, context and purpose(s) of Processing and the risks involved in the processing for the Data Subject. The Parties will in particular consider having recourse to encryption or Pseudonymisation, including during transmission, where the purpose of Processing can be fulfilled in that manner.
- (b) The Parties have agreed on the technical and organisational measures set out in ANNEX II. The data importer will carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

- (c) The data importer will ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (d) In the event of a Personal Data Breach concerning Personal Data Processed by the data importer under these Clauses, the data importer will take appropriate measures to address the Personal Data Breach, including measures to mitigate its possible adverse effects.
- (e) In case of a Personal Data Breach that is likely to result in a risk to the rights of natural persons, the data importer will without undue delay notify both the data exporter and the ADGM Commissioner of Data Protection pursuant to Clause 12. Such notification will contain:
 - (i) a description of the nature of the breach (including, where possible, categories and approximate number of Data Subjects and Personal Data records concerned);
 - (ii) its likely consequences;
 - (iii) the measures taken or proposed to address the breach; and
 - (iv) 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.
- (f) In case of a Personal Data Breach that is likely to result in a high risk to the rights of natural persons, the data importer will 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 paragraph (e), sub-paragraphs (ii) to (iv), unless the data importer has implemented measures to significantly reduce the risk to the rights of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer will instead issue a public communication or take a similar measure to inform the public of the Personal Data Breach.
- (g) The data importer will document all relevant facts relating to the Personal Data Breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Special Category Personal Data

- (a) Where the transfer involves Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, 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 or related security measures, the data importer will apply specific restrictions and additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the Personal Data, additional security measures (such as Pseudonymisation) and additional restrictions with respect to further disclosure.

8.7 Onward transfers

- (a) The data importer will not disclose the Personal Data to a third party located outside the ADGM (in the same jurisdiction as the data importer or in another jurisdiction,

“Onward Transfer”) unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an Onward Transfer by the data importer may only take place if:

- (i) it is to a jurisdiction benefitting from an adequacy decision pursuant to section 41 of the DPR 2021 that covers the Onward Transfer;
 - (ii) the third party otherwise ensures appropriate safeguards pursuant to sections 42 or 43 the DPR 2021 with respect to the Processing in question;
 - (iii) 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;
 - (iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
 - (v) it is necessary in order to protect the vital interests of the Data Subject or of another natural person; or
 - (vi) 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 or her of its purpose(s), the identity of the Recipient and the possible risks of such transfer to him or her due to the lack of appropriate data protection safeguards. In this case, the data importer will inform the data exporter and, at the request of the latter, will transmit to it a copy of the information provided to the Data Subject.
- (b) Any Onward Transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer will ensure that any person acting under its authority, including a Processor, Processes the data only on its instructions.

8.9 Documentation and compliance

- (a) Each Party will be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer will keep appropriate documentation of the Processing activities carried out under its responsibility.
- (b) The data importer will make such documentation available to the ADGM Commissioner of Data Protection on request.

Clause 8

Use of sub-Processors

- (a) *Not Used*
- (b) Where the data importer engages a sub-Processor to carry out specific Processing activities (on behalf of the Controller), it will 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 0. The data importer will ensure that the sub-Processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

- (c) The data importer will 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.
- (d) The data importer will 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 will notify the data exporter of any failure by the sub-Processor to fulfil its obligations under that contract.
- (e) The data importer will 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 will have the right to terminate the sub-Processor contract and to instruct the sub-Processor to erase or return the Personal Data.

Clause 9

Data Subject rights

- (a) The data importer, where relevant with the assistance of the data exporter, will deal with any enquiries and requests it receives from a Data Subject relating to the Processing of his or her Personal Data and the exercise of his or her rights under these Clauses without undue delay and at the latest within two months of the receipt of the enquiry or request. The data importer will take appropriate measures to facilitate such enquiries, requests and the exercise of Data Subject rights. Any information provided to the Data Subject will be in an intelligible and easily accessible form, using clear and plain language.
- (b) In particular, upon request by the data subject the data importer will, free of charge:
 - (i) provide confirmation to the Data Subject as to whether Personal Data concerning him or her is being Processed and, where this is the case, a copy of the data relating to him or her and the information in ANNEX I; 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 0; and provide information on the right to lodge a complaint with a Supervisory Authority in accordance with Clause 11(c)(i);
 - (ii) rectify inaccurate or incomplete data concerning the Data Subject;
 - (iii) 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.

- (c) Where the data importer Processes the Personal Data for direct marketing purposes, it will cease Processing for such purposes if the Data Subject objects to it.
- (d) The data importer will 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 or 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 will, where necessary in cooperation with the data exporter:
 - (i) inform the Data Subject about the envisaged Automated Decision, the envisaged consequences and the logic involved; and
 - (ii) implement suitable safeguards, at least by enabling the Data Subject to contest the decision, express his or her point of view and obtain review by a human being.
- (e) 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.
- (f) The data importer may refuse a Data Subject’s request if such refusal is allowed under the laws of the jurisdiction of destination and is necessary and proportionate to protect one of the objectives listed in section 21(1) of the DPR 2021.
- (g) If the data importer intends to refuse a Data Subject’s request, it will inform the Data Subject of the reasons for the refusal and the possibility of lodging a complaint with the ADGM Commissioner of Data Protection and seeking judicial redress.

Clause 10

Redress

- (a) The data importer will 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 will deal promptly with any complaints it receives from a Data Subject.
- (b) In case of a dispute between a Data Subject and one of the Parties as regards compliance with these Clauses, that Party will use its best efforts to resolve the issue amicably in a timely fashion. The Parties will keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) The data importer will abide by a decision that is binding under Applicable Law.

Clause 11

Liability

- (a) Each Party will be liable to the any other Party for any damages it causes the other Party by any breach of these Clauses.
- (b) Each Party will be liable to the Data Subject, and the Data Subject will 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 the liability of the data exporter under the DPR 2021.
- (c) 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 will be jointly and severally liable and the Data Subject is entitled to bring an action in court against any of these Parties.
- (d) The Parties agree that if one Party is held liable under paragraph (a), it will be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- (e) The data importer may not invoke the conduct of a Processor or sub-Processor to avoid its own liability.

Clause 12

Supervision

- (a) the data importer agrees to submit itself to the jurisdiction of and cooperate with the ADGM Commissioner of Data Protection 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 will provide the Supervisory Authority with written confirmation that the necessary actions have been taken.

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

Clause 13

Local laws and practices affecting compliance with the Clauses

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the jurisdiction 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 one of the objectives listed in section 1 of the DPR 2021, are not in contradiction with these Clauses.
- (b) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under

paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

- (c) Following a notification pursuant to paragraph (b), 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 will promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and data importer to address the situation. The data exporter will suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the ADGM Commissioner of Data Protection to do so. In this case, the data exporter will 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 these Clauses are terminated pursuant to this Clause, Clause 15(d) and Clause 15(e) will apply.

Clause 14

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

14.1 Notification

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
 - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the jurisdiction of destination for the disclosure of Personal Data transferred pursuant to these Clauses; such notification will include information about the Personal Data requested, the requesting authority, the legal basis for the request and the response provided; or
 - (ii) 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 will include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter or the Data Subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the jurisdiction 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 authorities, 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 ADGM Commissioner of Data Protection on request.

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

14.2 Review of legality and data minimisation

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer will, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It will not disclose the Personal Data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 13(b).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It will also make it available to the ADGM Commissioner of Data Protection on request.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 15

Non-compliance with the Clauses and termination

- (a) The data importer will promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter will suspend the transfer of Personal Data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 13(c).
- (c) The data exporter will be entitled to terminate the contract, insofar as it concerns the Processing of Personal Data under these Clauses, where:
 - (i) the data exporter has suspended the transfer of Personal Data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
 - (ii) the data importer is in substantial or persistent breach of these Clauses; or

- (iii) 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 will inform the ADGM Commissioner of Data of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal Data that has been transferred prior to the termination of the contract pursuant to paragraph (c) will at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same will apply to any copies of the data. The data importer will certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer will continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred Personal Data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only Process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where the ADGM Commissioner of Data Protection adopts a decision pursuant to section 41(3) of the DPR 2021 that covers the transfer of Personal Data to which these Clauses apply. This is without prejudice to other obligations applying to the Processing in question under the DPR 2021.

Clause 16

Governing law

These Clauses shall be governed by the law of the Abu Dhabi Global Market.

Clause 17

Choice of forum and jurisdiction

- (a) Any dispute arising from these Clauses shall be resolved by the courts of the Abu Dhabi Global Market.
- (b) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name: Nexpace Limited

Address: As specified in the MSU Open API Terms of Service (the “MSU API Terms”)

Contact person’s name, position and contact details: As specified in the MSU API Terms

Activities relevant to the data transferred under these Clauses: As specified in the MSU API Terms

Signature and date: The parties agree that the data importer’s acceptance of the MSU API Terms shall constitute execution of these Clauses by both parties.

Role (Controller/Processor): Controller

Data importer(s):

Name: As specified in the MSU API Terms

Address: As specified in the MSU API Terms

Contact person’s name, position and contact details: As specified in the MSU API Terms

Activities relevant to the data transferred under these Clauses: As specified in the MSU API Terms

Signature and date: The parties agree that the data importer’s acceptance of the MSU API Terms shall constitute execution of these Clauses by both parties.

Role (Controller/Processor): Controller

B. DESCRIPTION OF TRANSFER

1. Categories of Data Subjects whose Personal Data is transferred

Users of the MSU Community or Platform (as defined in the MSU API Terms) (i.e., natural persons who have connected their wallet to the Platform or MSU Community)

2. Categories of Personal Data transferred

Wallet address

In-game Identifiers (i.e., character ID, asset key)

Detailed NFT item information (including metadata for each item)

Digital Asset information associated

Marketplace activity/transaction data

※ While the above information may be publicly recorded on-chain or stored as off-chain game data, it may, in certain circumstances, be considered Personal Data under the ADGM Data Protection Regulations 2021, particularly where it can be linked, directly or indirectly, to an identifiable natural person.

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

Continuous, as determined by API calls initiated by the data importer (developer) during the development, integration, and operation of their applications or services developed using the MSU APIs or Synergy Apps.

4. Nature of the Processing

Retrieval of the above-listed Personal Data via the MSU API in order to integrate, display, and utilize such data within the importer's applications, services or Synergy Apps

Storage of such data in the developer's own systems (internal or third-party hosting) to enable the operation of the applications, services or Synergy Apps

Possible modification, sorting, or filtering of data for development, integration or operation of importer's the applications, services or Synergy Apps

Deletion or anonymization of such data upon the expiry of the retention period or termination of API access

5. Purpose(s) of the data transfer and further Processing

To enable the development, deployment, and operation of applications, services, or Synergy Apps that interact with and extend the MSU Community, allowing developers to provide users with a variety of features and information, including games, character management, item trading, balance display, and gameplay enhancements, and supporting the creation of functionality that is interoperable with the MSU Community

6. The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period

Retained for the duration of the importer's applications, services, or Synergy App's active integration with the MSU API and for as long as reasonably necessary to provide the services to end users, unless a shorter period is required under applicable law or by the MSU API Terms.

Upon termination of the MSU API Terms or withdrawal of API access, the importer/developer must delete or anonymize all Personal Data obtained via the API within thirty (30) days, or within a shorter period if specifically communicated to the importer by the exporter, unless retention is required by applicable law.

**ANNEX II- TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL
AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

The data importer will implement and maintain technical and organisational security measures that:

- (a) comply with the requirements of the ADGM Data Protection Regulations 2021; and
- (b) where specified by the data exporter, meet or exceed the standards set out in the data exporter's applicable security policies, provided that such policies are communicated to the data importer in advance.

The data importer shall also ensure that any Sub-processors engaged by it implement and maintain security measures that meet or exceed the same standards.

* * *