DATA PROTECTION AGREEMENT

concluded between

Affiliate Partner
with its registered Address
(hereinafter “Affiliate”)

on the one hand,

and

bet-at.home.com International Ltd.
Portomaso Business Tower
Level 12
STJ 4011, St. Julian’s, Malta
(hereinafter “bet-at-home” or “Advertiser”)

on the other hand,

Affiliate and Advertiser may hereinafter each be referred to as a "Party" and jointly the "Parties"

as follows:

1. BACKGROUND

Affiliate will integrate advertising material provided by Advertiser on its website. The Parties conclude an Affiliate Partner Agreement for this reason. To manage billing and payment by Advertiser's income access system, Affiliate will process personal data of Advertiser's customers. The Parties acknowledge that, for the purposes of this Agreement, they are each Controllers in the meaning of the Regulation (EU) 2016/679 (General Data Protection Regulation, "GDPR") with regard to the processing of personal data of data subjects. With respect to the separate controllership of Parties and without the intention of entering into a joint-controllership as defined in Article 26 GDPR, this Agreement sets out the framework for the sharing of personal data between the Parties and defines the principles and procedures that the Parties shall adhere to and the responsibilities the Parties owe to each other.

2. DEFINITIONS

Key Definitions are defined in the Affiliate Partner Agreement and in Article 4 GDPR and shall have the same meaning within this Agreement.

3. GUARANTIES

Parties will process personal data in compliance with all applicable laws, regulations, orders and similar legal acts. Parties especially guarantee that the processing of personal data will be conducted on the legal basis expressed in Article 6 GDPR.

Affiliate will process personal data generated on its website by cookies and tracking tools as a controller on its own and on its absolutely sole responsibility. Affiliate will obtain a valid consent for the processing of personal data where necessary.

Affiliate receives customer data plus gaming revenue data acquired through its affiliate websites. This data sharing solely serves accounting purposes to monitor compliance with the obligations of the Affiliate Partner Agreement. After review of the accounting – but no later than one month after the income/revenue data has been made available – Affiliate is obligated to provably delete the received data.

Parties will take appropriate technical and organizational measure against the unauthorised or unlawful processing of and against accidental loss, destruction or damage to personal data to ensure compliance with data protection laws.

Parties will notify each other immediately if they become aware of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data according to this Agreement and will provide such further information as the other Party may reasonably require and will provide such further information without undue delay and in any event within 24 (twenty-four) hours after identification of any potential or actual loss, together with all available information to document and report the incident.

It is the responsibility of each Party to ensure that its staff members are appropriately trained to handle and process the personal data in accordance with the technical and organisational security measures together with any other applicable data protection laws. The level, content and regularity of training shall be proportionate to the staff members' role, responsibility and frequency with respect to their handling and processing of the personal data.

Affiliate will hold harmless and indemnify Advertiser against any and all claims, actions, fines and other imposed sanctions subject to court or administrative proceedings or out of court settlements resulting from any processing activity exceeding the purpose of this Agreement, including, but not limited to all costs incurred in the defence of any claim, legal proceedings or other action brought against Advertiser.

4. APPOINTMENT OF PROCESSORS

Each Party may appoint one or more third party Processors to process the data on its behalf, provided that the Processor enters a written contract that conforms with all Data Protection Laws and this Agreement in all respects.

Each Party accept liability for all processing of the Data conducted by its Processors and for any breach of this Agreement that is caused by an act or omission of its Processors.

Each Party maintain a list of all Processors it appoints, including the processing activities they fulfil in respect of the processing relevant to this Agreement, and provides such list to the other Party upon request.

5. DATA TRANSFER OUTSIDE THE EU

If a Party processes data according to this Agreement outside the EU or the EEA, in a territory or sector that at the time is not subject to an EU Adequacy Decision, then it ensures that

- the data transfer and processing complies with Article 44 ff GDPR,
- only current EU SCCs are used,
- the recommendations from the document edpb, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, in the current version (currently version 2.0 of 18.06.2021) are observed.

6. CONFIDENTIALITY

The parties, their staff and third parties engaged by them are subject to an obligation of confidentiality with respect to the personal data, which are provided from Advertiser to Affiliate.

Affiliate may provide its staff and third parties engaged by it access to the personal data provided from Affiliate to Advertiser only insofar as it is absolutely necessary for achieving the purpose to this Agreement.

Parties shall impose on persons that are employed by them or that perform work on their behalf an obligation of confidentiality with respect to any personal data, which is provided from Advertiser to Affiliate, that may come to their knowledge.

The obligation of confidentiality shall survive the termination of this Agreement.

Parties shall notify each other of any request for access to, provision of or any other form of retrieval and disclosure of the personal data, unless such notification is prohibited by law on compelling grounds of public interest.

7. ASSISTANCE

Each Party acting as a Controller on its own, but will provide reasonable assistance to the other party as required in respect of

- dispute resolution with regards to personal data, if a data subject or a supervisory authority bring a dispute or claim concerning the processing of personal data against one or both Parties. The respective Party will inform each other about such disputes or claims and will cooperate with each other;
- personal data breaches;
- fulfilling data subjects' Rights.

8. MISCELLANEOUS

In the event of any conflict between the terms of this Data Protection Agreement and any provision of the Affiliate Partner Agreement and any other agreement between the Parties, this Data Protection Agreement shall prevail solely with respect to any data protection matters.

The provisions of this Data Protection Agreement are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision and the rest of this Data Protection Agreement shall remain in full force and effect.

Any amendment to this Data Protection Agreement must be made in writing upon mutual agreement by the Parties.

In the event of a breach of this Data Protection Agreement, the party that has complied with all the provisions of this Data Protection Agreement may terminate the Affiliate Partner Agreement and this Agreement with immediate effect.

SCHEDULE 1:
DETAILS ON DATA PROCESSING

1. NATURE ON DATA PROCESSING

Integrating advertising material on a website

2. PURPOSE ON DATA PROCESSING

Advertiser: Customer acquisition

Affiliate: monitoring compliance with the obligations of the Affiliate Partner Agreement

3. DATA SUBJECTS

Advertiser: potential players, Affiliate and Affiliate's service employee

Affiliate: Web users, Advertiser's service employee

4. PROCESSED DATA CATEGORIES

Advertiser and Affiliate:

- Player data
    - Player account number (=player name)
    - registration date
    - Player ID
    - Player country
- income/revenue data

Advertiser:

- Affiliate registration data
- sales data
- commission data
- data about ad performance

Affiliate (absolutely sole responsibility):

- Advertiser's service employee contact data
- Data generated by cookies and tracking tools

5. DATA PROCESSING DURATION

Data processing in general depends on the duration of the Affiliate Partner Agreement.

Retention Period of personal data usually depends on

- the registration platform,
- the Anti Money Laundering, Accounting and Responsible Gaming data retention obligations, depending on which obligation provides the longer retention period and
- Point 3 of the Data Protection Agreement.

SCHEDULE 2:
TECHNICAL AND ORGANISATIONAL MEASURES (HIGHLY RECOMMENDED)

1. PREVENTIVE SECURITY MEASURES – MEASURES TO PREVENT A SUCCESSFUL ATTACK

1.1. Technical measures

- **Logical access control:** Access rights are granted according to the "need-to-know" principle.
- **Authentication:** Personal data is accessible only after successful authentication.
- **Password security:** Passwords used for authentication consist of at least 8 characters, lower and upper case letters, numbers, and special characters. Passwords are stored encrypted only.
- **Encryption on the transmission path:** Personal data is encrypted if transmitted over the Internet, at least to the extent payroll data and sensitive data are concerned.
- **Encryption of mobile devices:** Mobile devices and mobile data carriers are encrypted, at least in case that payroll data or sensitive data are stored on these devices.
- **Network security:** A firewall is used that separates the internal network from the Internet and — as far as possible — blocks incoming network traffic.
- **Measures against malicious software:** Anti-virus software is used on all systems as far as possible. All incoming emails are automatically scanned for malicious software.
- **Management of security vulnerabilities:** To the extent feasible, the automatic installation of security updates is activated on all devices. Otherwise, critical security updates will be installed within 3 business days, medium-critical security updates will be installed within 25 business days, and non-critical security updates will be installed within 40 business days.

1.2. Organizational measures

- **Clear responsibilities:** Internal responsibilities for data security issues are defined.
- **Confidentiality requirements of employees:** Employees are obliged to maintain secrecy beyond the duration of their employment. In particular, employees may only transfer personal data to third parties upon the express instruction of a supervisor.
- **Training and information activities:** Employees are trained on data security issues (internally or externally) and adequately informed about data security issues (such as password security).
- **Orderly termination of employment relationships:** Upon termination of an employment relationship, all accounts of the leaving employee are immediately blocked for that employee and all keys of the leaving employee are collected.
- **Management of computer hardware:** Records are kept on the distribution of end devices to specific employees (e.g., PC, laptop, mobile phone).

- **Input control:** Control procedures are implemented to control the accuracy of personal data.
- **No duplicates of user accounts:** Each person should have their own user account — the sharing of user accounts is prohibited.
- **Limited use of administrative accounts:** User accounts with administrative rights are only used in exceptional cases — IT systems are normally used without administrative rights.
- **Selection of service providers:** When selecting service providers, the data security level offered by the service provider is taken into account. Service providers that are considered a processor are only used after execution of a processor agreement.
- **Secure data disposal:** Paper containing personal data is generally shredded or handed over to an external service provider for secure destruction. Media are completely overwritten or physically destroyed before being disposed of in order to prevent restoration of stored data.

1.3. Physical measures

- **Physical access control:** Access to business premises is only permitted for non-employees if accompanied by a company member.
- **Measures against burglary:** Access to business premises is equipped with adequate burglary protection (e.g., with security doors of higher safety classes).
- **Special protection of computer hardware:** Access to premises where computer servers are located is protected by special security measures (e.g., by additional locks).
- **Key management:** Keys that grant access to premises or parts thereof are only provided to particularly trustworthy persons, and only to the extent and as long as these persons require a separate key.

2. DETECTIVE SECURITY MEASURES — MEASURES TO DETECT AN ATTACK

2.1. Technical Measures

- **Scans for malware:** Scans for malware (anti-virus scans) are regularly performed to identify malicious software that has already compromised an IT system.
- **Automatic checks of log files:** To the extent that safety log files of several systems are collected on a centralized system, log files are automatically evaluated in order to detect possible security breaches.
- **Security mailing lists:** An employee of the company or an external service provider is required to subscribe to relevant mailing lists for the announcement of new IT security threats (e.g., mailing lists of the manufacturers of the software used) to recognize current threat situations.

2.2. Organizational measures

- **Employee security incident detection:** All employees are trained on the detection and reporting of security breaches (e.g., undetectable computer hardware, anti-virus software messages).
- **Reporting systems:** There are technical procedures in place that enable employees to report anomalies and anomalies in technical systems to the responsible persons.
- **External persons:** All employees are instructed to address non-employees should they be met on the premises.
- **Audits:** Audits are performed regularly (e.g., by verifying if all critical security updates have been installed). In particular, there is a regular check of access grants and access authorizations (which employee is assigned to which user account with which access rights, which persons have which keys).
- **Manual checking of log files:** Log files, if kept, are checked at regular intervals (e.g., with regard to unsuccessful authentication attempts).

2.3. Physical measures

- **Fire alarms:** To the extent appropriate with regard to the size and nature of the business facilities, fire alarms that are automatically triggered by smoke will be installed.

3. REACTIVE SECURITY MEASURES – RESPONSE TO AN ATTACK

3.1. Technical Measures

- **Data backup:** Data backups are created regularly and stored securely.
- **Data recovery concept:** A concept for the rapid restoration of data backups will be developed in order to allow for the timely restoration of regular operation after a security breach.
- **Automatic removal of malware:** The anti-virus software used automatically removes malware.

3.2. Organizational measures

- **Reporting obligation for employees:** All employees are instructed to immediately report security violations to a previously defined internal body or person.
- **Obligation to register external service providers:** All service providers are provided with contact details to report security breaches.
- **Incident response process:** Security breaches can be reported to the supervisory authority within 72 hours of knowledge of the breach via an appropriate reporting process. In particular, all employees will be provided with emergency telephone numbers of the persons that will have to get involved (e.g., emergency telephone number of the IT support).

3.3. Physical measures

- **Fire extinguishers:** There is a suitable number of fire extinguishers in the premises. All employees are aware of the location of these fire extinguishers.
- **Fire alarm:** In case that there is a fire detector that does not have an automatic connection to the fire department, an appropriate process ensures that the fire department can be contacted manually.

4. DETERRENT SECURITY MEASURES – MEASURES TO REDUCE ATTACK MOTIVATION

4.1. Technical Measures

- **Automatic alerts:** Users receive automatic alerts on risk-entailing IT use (such as through the web browser if an encrypted web site does not use correct SSL / TLS certificates).

4.2. Organizational measures

- **Sanctions in the case of attacks by own employees:** All employees are informed that attacks on company-owned IT systems are not tolerated and that such attacks may result in serious consequences under employment law, particularly including dismissal.
- **Logging of access:** Any access to applications, in particular input, deletion and modification of data, is logged.

SCHEDULE 3:
CONTROLLER TO CONTROLLER STANDARD CONTRACTUAL CLAUSES (ONLY REQUIRED, IF AFFILIATE IS NOT SETTLED IN EU OR EEA OR IF THERE IS NO ADEQUACY DECISION OF EUROPEAN COMMISSION)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

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

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

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

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

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

Clause 2

Effect and invariability of the Clauses

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

do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3

Third-party beneficiaries

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

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.5 (e) and 8.9(b);

(iii) Clause 12(a) and (d);

(iv) Clause 13;

(v) Clause 15.1(c), (d) and (e);

(vi) Clause 16(e);

(vii) Clause 18(a) and (b).

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

(a) 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 the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, 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 Annex I.A.

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

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.

8.1 Purpose limitation

The data importer shall 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:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall 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;

(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) 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.

(c) On request, the Parties shall 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 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.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall 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 shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall 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.

8.5 Security of processing

(a) 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 state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall 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 shall 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 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 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 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 paragraph (e), points ii) to iv), 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.

(g) 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.

8.6 Sensitive data

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

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") 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 country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

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

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 shall 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 shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

[Clause 9]

[Intentionally omitted]

Clause 10

Data subject rights

(a) 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 without undue delay and at the latest within one month of the receipt of the enquiry or request. 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.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) 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 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 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(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 shall cease processing for such purposes if the data subject objects to it.

(d) 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:

(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/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 country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 11

Redress

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

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

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

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

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

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

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

Clause 12

Liability

(a) 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.

(b) 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 the liability of the data exporter under Regulation (EU) 2016/679.

(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 shall 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 (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.

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

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries,

submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

(i) 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;

(ii) 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;

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

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

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

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

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

data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1 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 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

(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 shall include all information available to the importer.

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

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

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

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do

so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

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

(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 16

Non-compliance with the Clauses and termination

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

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

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

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

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii)

Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Malta.

Clause 18

Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts of Malta.

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

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

APPENDIX

EXPLANATORY NOTE:

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

ANNEX I

A. LIST OF PARTIES

See cover of the Data Protection Agreement

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

See Schedule 1 of the Data Protection Agreement

……..

Categories of personal data transferred

See Schedule 1 of the Data Protection Agreement

……..

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

-

……..

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

continuous

……

Nature of the processing

See Schedule 1 of the Data Protection Agreement

……

Purpose(s) of the data transfer and further processing

See Schedule 1 of the Data Protection Agreement

……..

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

See Schedule 1 of the Data Protection Agreement

……..

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

Transfer to service provider who supports Advertiser or Affiliate in performing the above mentioned purpose of processing within the above mentioned duration.

……..

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Malta

……..

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

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

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.

See Schedule 2 of the Data Protection Agreement

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

See Schedule 2 of the Data Protection Agreement

SCHEDULE 4:
SUPPLEMENTARY MEASURES TO THE STANDARD CONTRACTUAL CLAUSES (ONLY ACCESSIBLE, IF AFFILIATE IS NOT SETTLED IN EU OR EEA OR IF THERE IS NO ADEQUACY DECISION OF EUROPEAN COMMISSION)

1. PLACE OF DATA PROCESSING

(1)If data importer operates a subsidiary entertainment within the EEA, personal data will be processed at this subsidiary entertainment.

(2)If data processing within the EEA is not possible, data importer shall inform data exporter about the reasons as follows:

a. The data protection officer, if existent, shall be provided with all the relevant information prior to the transfer to the third country, and shall be consulted on the necessity of the transfer and the additional safeguards, if any.

b. Relevant information should include, for example, the assessment on the necessity of the transfer to the third country of the specific personal data, an overview of the laws of the destination country applicable and the safeguards the importer committed to implement (certifications).

2. DATA SUBJECT RIGHTS

Personal data transmitted in plain text in the normal course of business (including in support cases) shall only be accessed to public authorities with the express or implied consent of the data exporter and/or the data subject.

3. (SUB-) PROCESSORS

(1)If data importer transfers personal data to (sub-) processors, it ensures, that data transfer and data processing complies with edpb, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0.

(2)Data minimisation should be considered in this regard, in order to limit the exposure of personal data to unauthorised access.

4. TRANSPARENCY OBLIGATIONS

4.1. Information about access by public authorities to the transferred data

Read in conjunction with Clause 15 standard contractual clauses 2021/914 the importer is required to:

(1) enumerate the laws and regulations in the destination country applicable to the data importer or its (sub-) processors that would permit access by public authorities to the personal data that are subject to the transfer, in particular in the areas of intelligence, law enforcement, administrative and regulatory supervision;

(2) in the absence of laws governing the public authorities' access to data mentioned under (1), provide information and statistics based on the importer's experience or reports from various sources (e.g. partners, open sources, national case law and decisions from oversight bodies) on access by public authorities to personal data in situations of the kind of the data transfer at hand (i.e. in the specific regulatory area; regarding the type of entities to which the data importer belongs, etc.);

(3) indicate which measures are taken to prevent the access to the provided data by public authorities;

(4) provide sufficiently detailed information on all requests of access to personal data by public authorities which the importer has received over a specified period of time, in particular in the areas mentioned under (1) above and comprising information about the data requested, the requesting body and the legal basis for disclosure and to what extent the importer has disclosed the data request;

(5) specify whether and to what extent the importer is legally prohibited to provide the information mentioned under (1) – (4) above.

4.2. Information on back doors

The data importer certifies that

(1) it has not purposefully created back doors or similar programming that could be used to access the system and/or personal data by third parties,

(2) it has not purposefully created or changed its business processes in a manner that facilitates access to its systems or personal data by third parties, AND

(3) national law or government policy does not require the importer to create or maintain back doors or to facilitate access to its systems or personal data by third parties or to hand over encryption keys.

4.3. legal and policy developments monitoring

(1) The data importer shall monitor any legal und policy developments that might lead to its inability to comply with its obligations, and promptly inform the data exporter of any such changes and developments, ahead of their implementation to enable the data exporter to recover the data from the data importer.

(2) The data importer shall implement one-click-solutions to promptly secure or return personal data to the data exporter, or if this is not feasible, delete or securely encrypt personal data in case of an inspection by public authorities; in case of significant legal or policy developments the data importer will use this one-click-solutions without necessarily waiting for the data exporter's instructions.

(3) In case of an infringement of this clause data exporter may terminate the Affiliate Partner Agreement and the Data Protection Agreement with immediate effect.

5. OBLIGATIONS TO TAKE SPECIFIC ACTIONS

5.1. Review

(1) The data importer shall review, under the law of the country of destination, the legality of any order to disclose data, notably whether it remains within the powers granted to the requesting public authority.

(2) The data importer shall challenge any order to disclose data if, after a careful assessment, it concludes that there are grounds under the law of the country of destination to do so.

(3) When challenging an order to disclose data, the data importer shall seek interim measures to suspend the effects of the order until the court or the authority has decided on the merits.

(4) In case of an order to disclose data data importer shall follow Clause 15 standard contractual clauses 2021/914 and shall not disclose the personal data requested until required to do so under the applicable procedural rules.

(5) The data importer shall only provide the minimum amount of information when responding to the order to disclose data, based on a reasonable interpretation of the order.

5.2. Information of incompatibility

In the situation described in 5.1 the data importer shall inform the requesting public authority of the incompatibility of the order with the safeguards contained in the Article 46 GDPR transfer tool and the resulting conflict of obligations for the data importer.

6. INTERNAL POLICIES FOR GOVERNANCE OF TRANSFERS

(1) Data importer shall implement adequate internal policies with clear allocation of responsibilities for data transfers, reporting channels and standard operating procedures for cases of covert or official requests from public authorities to access the data.

(2) These policies shall include, among others, the appointment of a specific team, composed by experts on IT, data protection and privacy laws, to deal with requests that involve personal data transferred from the EU; the notification to the senior legal and corporate management and to the data exporter upon receipt of such requests; the procedural steps to challenge disproportionate or unlawful requests and the provision of transparent information to data subjects.

(3) Data importer shall submit these policies to data exporter.

7. TRANSPARENCY AND ACCOUNTABILITY MEASURES

Data importer shall document and record the requests for access received from public authorities and the response provided as well as the actions taken, alongside the legal reasoning and the actors involved (e.g. if the exporter has been notified and its reply, the assessment of the team in charge of dealing with such requests, etc.). These records shall be made available to the data exporter, who can in turn provide them to the data subjects concerned.