DATA PROCESSING AGREEMENT

1. INTRODUCTION

1.1 This NetRefer Data Processing Agreement ("**DPA**" or "**Data Processing Agreement**") reflects the Parties' agreement with respect to the terms governing the Processing of Personal Data in accordance with the Data Protection Laws and constitutes an integral part of the NetRefer Terms of Service ("**TOS**"). This DPA will control with respect to the subject matter herein in the event of any conflict with the TOS.

1.2 In all cases, Licensor ("**Processor**"), or a third party acting on behalf of Processor, acts as the Processor of Personal Data, and Licensee ("**Controller**") remains Controller of Personal Data as per the Data Protection Laws. The term of this DPA shall run concurrently to the term of the Order Form.

1.3 Terms not otherwise defined herein shall have the meaning as set forth in the TOS.

1.4 This DPA includes the following Appendices:

(i) Security layers and methodologies applied at infrastructure layer, attached hereto as **Appendix A**.

(ii) Security mechanisms for the protection of data access at Application layer, attached hereto as **Appendix B**.

(iii) Security processes at an operational layer, attached hereto as **Appendix C**.

(iv) Processing Activities, attached hereto as **Appendix D**.

(v) Contact details of the Data Processor, attached hereto as **Appendix E**.

(vi) List of Sub-Processors, as may be updated from time to time, referred to as **Appendix F**, and which is accessible by clicking on the hyperlink provided.

2. DEFINITIONS

2.1 "**Controller**", "**Data Subject**", "**Personal Data**", "**Processing**", "**Processor**", "**Special Categories of Data**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR;

2.2 "**Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR, and all other applicable laws and regulations relating to the Processing of Personal Data and privacy;

2.3 "**GDPR**" means EU General Data Protection Regulation 2016/679;

2.4 "**Sub-Processor**" means any processor engaged by the Processor or by any other sub-processor of the Processor who agrees to receive from the Processor or from any other sub-processor of the Processor Personal Data exclusively intended for Processing activities to be carried out on behalf of the Processor after the transfer in accordance with his instructions;

2.5 "**Technical and Organisational Security Measures**" means those measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the Processing involves the transmission of Personal Data over a network, and against all other unlawful forms of processing.

3. SCOPE AND RESPONSIBILITY

3.1 Processor shall process Personal Data on behalf of Controller. Controller and Processor shall be separately responsible for conforming with such statutory data protection regulations as are applicable to them.

3.2 Based on this responsibility, Controller shall be entitled to demand support towards the rectification, deletion, blocking and making available of Personal Data during the term of the TOS

in accordance with the further specifications of such agreement on return and deletion of Personal Data.

3.3 The regulations of this DPA shall equally apply if testing or maintenance of automatic processes or of Processing equipment is performed on behalf of Controller, and access to Personal Data in such context cannot be excluded.

3.4 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Controller and the Processor shall implement appropriate Technical and Organisational Security Measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4. OBLIGATIONS OF PROCESSOR

4.1 Processor shall collect, process and use Personal Data only within the scope of Controller's instructions and for the fulfilment of the services contracted. If the Processor thinks that an instruction of the Controller infringes the Data Protection Laws or other data protection provisions, the Processor shall inform the Controller and reserves the right to refuse executing such instruction.

4.2 Within the Processor's area of responsibility, Processor shall structure Processor's internal corporate organisation to ensure compliance with the specific requirements of the protection of Personal Data. Processor shall take the appropriate Technical and Organisational Security Measures to adequately protect Controller's Personal Data against misuse and loss in accordance with the requirements of the Data Protection Laws. Such measures hereunder shall include, but not be limited to:

a) the prevention of unauthorised persons from gaining access to Personal Data Processing systems (physical access control);

b) the prevention of Personal Data Processing systems from being used without authorisation (logical access control);

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

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

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

f) ensuring that Personal Data is processed solely in accordance with the Processing activities stipulated in Appendix D attached hereto;

g) ensuring that Personal Data are protected against accidental destruction or loss (availability control).

4.3 Processor and each of its Sub-Processors shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Controller's Personal Data. Processor shall ensure that any personnel or Sub-Processors entrusted by the Processor with Processing Controller's Personal Data have undertaken to comply with the principle of data secrecy in accordance with the Data Protection Laws and have been duly instructed on the protective regulations of the Data Protection Laws. The undertaking to secrecy shall continue after the termination of the above-entitled activities.

4.4 Processor shall, without undue delay, inform Controller in case of a serious interruption of operations or violations by the Processor or persons employed by it of provisions to protect Personal Data or of terms specified in this DPA. In such an event, Processor shall implement the measures necessary to secure the Personal Data and to mitigate potential adverse effects on the Data Subjects and shall agree upon the same with Controller without undue delay. Processor shall support Controller in fulfilling Controller's disclosure obligations.

4.5 The Controller shall retain title as to any carrier media provided to Processor as well as any copies or reproductions thereof. Processor shall store such media safely and protect them against unauthorised access by third parties for the amount of time specified within the Data Retention Policy.

4.6 Processor shall, upon Controller's request, provide without undue delay to Controller all information on Controller's Personal Data and information. Processor shall be obliged to securely delete any data based on an instruction issued by Controller on a case-by-case basis. Where Controller so decides, Processor shall hand over such data to Controller or store it on Controller's behalf as per the Data Retention Policy issued by the Processor.

4.7 The Processor shall promptly notify the Controller about:

(a) any legally binding request for disclosure of the Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation; and

(b) any accidental or unauthorised access; and

(c) any request received directly from the Data Subjects without responding to that request, unless it has been otherwise authorised to do so by the Controller.

4.8 The Processor shall deal without undue delay with all inquiries from the Controller relating to its Processing of the Personal Data subject to this DPA and shall abide by the advice of the Supervisory Authority with regard to the Processing of the Personal Data transferred.

4.9 The Processor will ensure that in case of Sub-Processors, the Processing services by the Sub-Processor will be carried out in accordance with the Data Protection Laws.

4.10 The Processor shall promptly inform the Controller of any terminated employees with access credentials to the Controller's internal or data systems, in order for the Controller to block access and take the necessary security precautions.

4.11 The Processor shall provide the Controller with all information necessary to demonstrate compliance with this DPA and the Data Protection Laws upon request.

4.12 The Processor shall ensure that any Personal Data shall be disclosed only when necessary, to authorised personnel who are duly bound by confidentiality agreements.

5. OBLIGATIONS OF CONTROLLER

5.1 Controller shall inform Processor without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the Processing of Personal Data detected during a verification of the results of such Processing.

5.2 Controller shall be responsible for notifying Data Subjects of a data breach or for a request from the Data Subject themselves or for a corresponding provision of an otherwise applicable national data protection law.

5.3 Controller shall, upon termination or expiration of the TOS and by way of issuing an instruction, stipulate, within a reasonable period of time set by Processor, the reasonable measures to return data carrier media or to delete stored data. In the case of no instructions being issued within 30 days, the Processor will anonymize the Personal Data and retain it in accordance with the Data Retention Policy. Non-personal data shall be retained by Processor in accordance with its commercial requirements.

5.4 Any additional cost arising in connection with the return or deletion of Personal Data after the termination or expiration of the TOS shall be borne by Controller.

5.5 The Controller agrees and warrants that it will ensure compliance with the security measures and security processes defined by the Processor.

5.6 The Controller shall ensure that the Personal Data which it supplies or discloses to the Processor has been obtained fairly and lawfully. The Controller agrees and warrants that if the transfer involves Special Categories of Data, the data has been collected with the Data Subject's explicit and recorded consent resulting from a specific action as silence or inaction do not constitute consent.

5.7 The Controller shall ensure (and put in place all necessary measures to ensure) that any login details provided or created for the purpose of accessing Processor's systems are kept confidential, safe and secure at all times.

5.8 The Controller shall promptly inform the Processor of any terminated employees with access credentials to the Processors' internal or data systems, in order for the Processor to block access and take the necessary security precautions.

6. ENQUIRIES BY DATA SUBJECTS TO CONTROLLER

6.1 Where Controller, based upon applicable Data Protection Laws, is obliged to provide information to an individual about the collection, Processing or use of its Personal Data, Processor shall assist Controller in making this information available, provided that:

(a) Controller has instructed Processor in writing to do so, and

(b) Controller reimburses Processor for the costs arising from this assistance.

6.2 Where a Data Subject requests the Processor to correct, delete or block Personal Data, Processor shall refer such Data Subject to the Controller and notify the Controller of such requests.

6.3 Processor must notify Controller of a Data Subject's request regarding the exercise of the Data Subject's right.

7. SUB-PROCESSORS

7.1 Processor shall be entitled to subcontract Processor's obligations for the fulfilment of the Processing services to the Sub-Processors and third parties that are listed in Appendix F, as may be amended from time to time.

7.2 If the Processor updates the Sub-Processors listed in Appendix F, the Processor must notify the Controller thereof in writing (email to the email address(es) on record in Processor's account information for Controller is sufficient) and the Controller shall have the right to object thereto within 14 days after being notified. The objection must be based on reasonable grounds (e.g. if the Controller proves that significant risks for the protection of its Personal Data exist at the Sub-Processor). If the Processor and Controller are unable to resolve such objection, the Controller may terminate the Agreement, as described in the TOS.

7.3 Processor remains liable for the acts and omissions of its Sub-Processor.

8. DATA RETENTION POLICY

8.1 This data retention policy is the Processor's established protocol for retaining information for operational or regulatory compliance needs.

8.2 The scope of this document is limited to data in relation to the systems provided by the Processor to the Controller and communication between these two parties.

8.3 For the duration of the Agreement (as defined in the TOS), the data provided to the Processor will be retained and processed for the performance of, and in line with, the Agreement. This data may include Personal Data which is used to provide the Processing activities referred to in Appendix D and for the fulfilment of the TOS. Upon termination of the Agreement, the Controller may request the Processor to return and/or delete any Personal Data that it retains. Unless such request is received, the Processor reserves the right to retain the Personal Data for the integrity of data

within the systems and/or for statistical purposes, where such Personal Data shall be archived in an aggregated and obfuscated form to preserve the anonymity of the Data Subject.

8.4 The retention periods are based on the legitimate interest of the Processor. Should the relevant interest, legislation, laws or regulation be updated or modified, the retention periods shall be adjusted accordingly for the purpose of compliance.

9. TRANSFER OF PERSONAL DATA

9.1 The Processor shall not transfer any Personal Data processed on behalf of the Controller to a third country outside the EEA without prior consent of the Controller.

9.2 The Parties shall ensure that, to the extent that any Personal Data is transferred to a third country outside the EEA that has not received a binding adequacy decision by the European Commission, such transfer shall be subject to an appropriate transfer mechanism that provides an adequate level of data protection in accordance with the Data Protection Laws.

10. DUTIES TO INFORM, ADDITIONAL TERMS

10.1 Where Controller's Personal Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while being processed, Processor shall inform Controller without undue delay. Processor shall, without undue delay, notify to all pertinent parties in such action, that any Personal Data affected thereby is in Controller's sole property and area of responsibility, that Personal Data is at Controller's sole disposition, and that Controller is the responsible body in the sense of the Data Protection Laws.

10.2 Where individual regulations of this DPA are invalid or unenforceable, the validity and enforceability of the other regulations of this DPA shall not be affected.

11. RETURN OR DESTRUCTION OF PERSONAL DATA

11.1 Upon termination of this Data Processing Agreement and upon the Controller's written request, the Processor shall either delete or return all Personal Data to the Controller. Unless otherwise stated by the Controller in the decommissioning process, the Processor reserves the right to retain the data for integrity of data within the systems and for statistical purposes, where such data shall be archived in an aggregated and obfuscated state to preserve the anonymity of the Data Subject.

11.2 Where applicable, the Processor shall notify all relevant third parties supporting its own Processing of the Personal Data of the termination of the Data Processing Agreement and shall ensure that all such third parties either destroy the Personal Data or return the Personal Data to the Controller, at the discretion of the Controller.

12. AUDIT OBLIGATIONS

12.1 The Processor shall endeavour to carry out an audit of compliance through a penetration test, the results of which may be shared with the Controller upon request.

12.2 In the case where an audit of the Processor is required by the Controller for the fulfilment of a legal requirement:

(a) Controller shall have the right to access the Processor's premises to audit compliance by the Processor of the provisions of this Data Processing Agreement. If a third party is to conduct such audit, the audit needs to be conducted by a third -party auditor agreed upon by both Parties.

(b) Any audits are to take place during the Processor's normal business hours, and upon reasonable and prior written notice.

(c) All costs related to auditors' fees are to be borne by the Controller.

(d) The Processor shall fully cooperate with the Controller and/or the designated third party and shall provide the Controller and/or third party with any access, information and documents reasonably requested.

12.3 In the event that the audit reveals any non-compliance by the Processor with the provisions of this Data Protection Agreement or any national or European Data Protection Laws and regulations, the Processor shall without undue delay implement the necessary corrective measures, at its own expense.

13. LIABILITY

13.1 A Data Subject who has suffered material or non-material damage as a result of an infringement of GDPR or this DPA, may receive compensation from the Controller or Processor for the damage suffered.

13.2 The Processor shall be liable for the damage caused by the Processing of Personal Data only where it has not complied with obligations of GDPR specifically directed to processors or with this DPA or where it has acted outside or contrary to lawful written instructions of the Controller.

13.3 The Controller shall be liable for damages to Data Subjects which are caused by the Processing of Personal Data which is not compliant with the Data Protection Laws and which are not caused by the Processor's acts or omissions.

13.4 Except as specifically stated in this clause above, the liability of Processor and Controller are as defined in the TOS.

14. MISCELLANEOUS PROVISIONS

This Data Processing Agreement contains the entire agreement and understanding between the Parties with respect to the subject matter hereof and supersedes and replaces all prior agreements or understandings, written or oral, with respect to the same subject matter still in force between the Parties.

The Processor reserves the right to change and update this DPA at any time, provided that:

(i) Changes are in compliance with European and local laws and regulations; and
(ii) Written notice is provided to the Controller.

Appendix A: Security layers and methodologies applied at infrastructure layer

Network Edge Traffic Monitoring & Mitigation

Simulated & Vetted through Penetration Testing

- Comprehensive traffic monitoring
- Multi-layered Approach
    - Network-level packet scanning
    - Server-level anomaly detection
- Constant Learning Patterns
- Automated Mitigation
- On-Edge Packet Analysis
- DDoS protection
- Load Balancing Mechanisms
- Performance Caching Techniques
- Web Application Firewall

Perimeter Network Security – Firewall

- Enforced Policy
- Restriction of services
- Last rule set to DROP unwanted packets
- Restrict inbound UDP traffic
- Up-to-date software revisions
- Service packs and patching
- Access Log (Default Retention Policy – Overwrite)
- Change Log (Default Retention Policy – Overwrite)
- Authorized Approval of any changes or maintenances

Remote Access Methods

- L2TP/IPSec tunnel VPN protocol
- Data Encrypted in transit
- Access Log (Default Retention Policy – Overwrite)
- Change Log (Default Retention Policy – Overwrite)
- Management Approval

Network Routers & Switches

- Up-to-date software versions
- Out-of-band connectivity not permitted
- 2-factor Auth for in-band access routers
- NAT translations logs (Default Retention Policy – Overwrite)
- Access Log (Default Retention Policy – Overwrite)
- Change Log (Default Retention Policy – Overwrite)

Systems Security Access Controls

- Managed Active Directory Services
- Enforced Group Policies (e.g. Password complexity / Failed Login Attempts)
- Maintain list of personnel (High-Level system privileges / least privileges)
- Quarterly User Access Review

Application Security (Operating Systems / Hosting)

- Quarterly Security Risk Assessment using Netcraft
- New release deployment cycle is assessed using ZAP
- High Vulnerabilities Review Process
- Monthly Patching Maintenance (Only applicable and approved updates)
- Real-time Virus Protection (Across all servers and on user workstations)
- Servers hardening prior to presenting on the network
- Formal process for securely wiping data

Incident Response (Internal Procedures to report on the below scenarios)

- Suspected Security Vulnerabilities
- Network Intrusion
- Data/Information Theft
- Unauthorised Data Access
- Equipment Theft
- External Threats to the site
- Physical Intrusion

Business Continuity Plan

- High Availability Approach
- Geographically independent environment to act as Disaster Recovery
- Quarterly testing of Ad serving application
- Offsite backups of application binary files / configs / media files / scripts
- Documented Process of invoking DR
- Multiple ISP providers
- RTO 30 minutes
- RPO last minute

Appendix B: Security mechanisms for the protection of data access at application layer

- All authentication communication for all application entry points is handled over secure communication;
- Authorisation is built around a role -based access control extended through a privilege framework;
- All application data is protected adopting the least privilege principle using encryption, data masking and obfuscation as supporting mechanisms where applicable;
- Application level auditing is implemented throughout which is also strengthened via database level auditing for data sets requiring complete DML traceability where applicable.

It is the responsibility of the Controller to conduct a due diligence and implement any additional safeguards as required for systems provided by NetRefer which the Controller is accessing, operating as well as hosting (acting as a Processor).

Appendix C: Security processes at an operational layer

- All NetRefer employees are required to sign non-disclosure agreements upon employment.
- All NetRefer employees pass through a criminal background and reference check prior to being employed.
- All NetRefer employees are given an overview of the GDPR upon joining and subsequently a refresher on an annual basis.
- All NetRefer partners & suppliers go through a due diligence process from both an operational and security perspective.
- NetRefer partners & suppliers are required to sign non-disclosure agreements.
- All company policies and processes are reviewed by the Governance, Risk and Compliance department to ensure both cohesiveness and compliance to security standards and regulatory compliance prior to being deployed.
- All company policies and processes are reviewed and audited annually by the Governance, Risk and Compliance department to ensure compliance.
- Processes are in place to ensure penetration testing is carried out on a regular basis by an independent 3rd party.
- NetRefer employs the least privilege principle across all its systems including internal ones.
- NetRefer has processes in place to ensure regular security patching of all systems.
- NetRefer has systems and processes in place for the monitoring of critical functions.
- NetRefer has a clean desk policy and shredding policies.
- NetRefer has strict policies for communication of credentials.
- NetRefer has automated policies preventing the use of mass storage devices such as USBs or external hard disks.
- NetRefer implements hard disk encryption on all company laptops and machines.
- NetRefer has in place manual processes to cater for the right of access, portability and right to be forgotten which are triggered upon request via the customer portal.
- NetRefer has in place internal processes to ensure adherence to its Data Retention Policy.

Appendix D: Processing Activities

Data Types	Grounds for Processing
Affiliate sign up data	Account management and providing access to the Affiliate Management System.
Affiliate Managers sign up data	Account Management and providing access to the Administration interface of the Performance Marketing Platform.
Customer Registration data	Used to associate the player with the affiliate and verify the acquisition of the customer for the purpose of calculating the affiliate rewards.
Transactional Activity	Processed and aggregated for the purpose of calculating the affiliate rewards.
Affiliate payment information	Processed for the purpose of generating the payment files for affiliates.
Marketing media views and clicks	Processed for the purpose of ▪ tracking, media, campaign and affiliate performance. ▪ Linking a customer to an affiliate ▪ Rewarding affiliates
Affiliate, Customer, Views, Clicks and rewards	Generation of statistics, performance metrics and KPIs for ▪ Affiliate management ▪ Affiliate performance ▪ Rewarding ▪ Financial reporting ▪ Benchmarking
All data within the systems	For the purposes of executing the Controller's instructions, and affecting system and infrastructure maintenance, software updates and upgrades.
Controller's Employee basic data	For the purpose of providing credentials to internal NetRefer support tools and mechanisms.

Appendix E: Contact details of the Data Processor

NetRefer monitors compliance with its data protection policies and procedures and has procedures to address privacy-related complaints and disputes. In this regard, individuals may address their data protection related concerns by contacting NetRefer on dpo@netrefer.com or +356 2767 3337.

NetRefer shall respond to all inquiries, concerns and/or complaints about its personal information handling practices.

The regulatory body in Malta responsible for the handling of personal information is the Office of the Information and Data Protection Commissioner. For more information, please visit https://idpc.org.mt/en/Pages/Home.aspx

Every privacy-related complaint will be acknowledged, recorded and investigated, and the results of the investigation will be provided. If a complaint is found to be justified, appropriate measures will be taken including, if necessary, amending our privacy policies and procedures.

Appendix F: List of Sub-Processors

Please click on **Appendix F** to access the list of Sub-Processors used by NetRefer.