NetRefer

Data Processing Agreement

A SIGNED COPY OF THIS DPA IS AVAILABLE UPON REQUEST

This Data Processing Agreement and its Annexes ("**DPA**") reflects the parties' agreement with respect to the processing of personal data by Arnold Media Limited t/a NetRefer on behalf of the Client, in connection with the Service under the Agreement.

This DPA is supplemental to, and forms an integral part of, the Agreement. In case of any conflict or inconsistency with the terms of the Agreement, this DPA will take precedence over the terms of the Agreement to the extent of such conflict or inconsistency.

The term of this DPA will follow the term of the Agreement.

Terms not otherwise defined in this DPA will have the meaning as set forth in the Agreement.

For transfers to non-EU controllers, the Standard Contractual Clauses set forth in this DPA below shall also apply.

Section I

Clause 1 - Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) 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.

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2 – Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3 – Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, 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 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4 – Hierarchy

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

Clause 5 – Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

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

Section II – Obligations of the Parties

Clause 6 – Description of Processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7 – Obligations of the Parties

7.1 Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

(c) If the processor becomes aware that it cannot process personal data in accordance with the controller's Instructions due to a legal requirement under any applicable law, the processor will (i) promptly notify

the controller of that legal requirement to the extent permitted by the applicable law; and (ii) where necessary, cease all processing (other than merely storing and maintaining the security of the affected personal data) until such time as the controller issues new Instructions with which the processor is able to comply. If this provision is invoked, the processor will not be liable to the controller under the Agreement for any failure to provide the Service until such time as the controller issues new lawful Instructions with regard to the processing.

(d) The parties agree that the Agreement (including this DPA), together with the controller's use of the Service in accordance with the Agreement, constitutes the controller's complete instructions to the processor in relation to the processing of personal data, so long as the controller may provide additional instructions during the term of the Agreement that are consistent with the Agreement, the nature and lawful use of the Service.

(e) The controller shall ensure that the personal data which it supplies or discloses to the processor has been obtained fairly and lawfully.

7.2 Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3 Duration of the processing of Personal Data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4 Security of Processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) 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.

(d) 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.

(e) The controller is responsible for independently determining whether the data security provided for in the Service adequately meets its obligations under applicable data protection laws. The controller is also responsible for its secure use of the Service, including protecting the security of personal data in transit to and from the Service (including to securely backup or encrypt any such personal data).

(f) Notwithstanding any provision to the contrary, the processor may modify or update the security measures in Annex III at its discretion provided that such modification or update does not result in a material degradation in the protection offered by the said security measures.

7.5 Sensitive Data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

The controller agrees and warrants that if the transfer involves sensitive 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.

7.6 Documentation and Compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

(f) All costs related to auditors' fees are to be borne by the controller.

(g) In the event that the audit reveals any non-compliance by the processor with the provisions of this DPA 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.

(h) 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.

(i) Within the scope of the Agreement and in using the Service, the controller will be responsible for complying with all requirements that apply to it under applicable data protection laws with respect to its processing of personal data and the Instructions it issues to the processor.

(j) In particular but without prejudice to the generality of the foregoing, the controller acknowledges and agrees that it will be solely responsible for: (i) the accuracy, quality, and legality of personal data and the means by which it acquired personal data; (ii) complying with all necessary transparency and lawfulness requirements under applicable data protection laws for the collection and use of the personal data, including obtaining any necessary consents and authorizations; (iii) ensuring it has the right to transfer, or provide access to, the personal data to the processor for processing in accordance with the terms of the Agreement (including this DPA); (iv) ensuring that its instructions to the processor regarding the processing of personal data comply with applicable laws, including data protection laws; and (v) complying with all laws (including data protection laws) applicable to any emails or other content created, sent or managed through the Service, including those relating to obtaining consents (where required) to send emails, the content of the emails and its email deployment practices.

7.7 Use of Sub-Processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least ten (10) days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

If the controller does notify the processor of such an objection, the parties will discuss the controller's concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, the processor will, at its sole discretion, either not appoint the new sub-processor, or permit the controller to suspend or terminate the Agreement in accordance with the termination provisions of the Agreement without liability to either party (but without prejudice to any fees incurred by the controller prior to suspension or termination).

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8 International Transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7 for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8 – Assistance to the Controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.

The controller shall reimburse the processor for the commercially reasonable costs arising from this assistance.

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9 – Notification of Personal Data Breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

9.3 Liability

(a) 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.

(b) 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 where it has acted outside or contrary to lawful written instructions of the controller.

(c) The controller shall be liable for damages to data subjects which are caused by the processing of personal data which is not compliant with GDPR and which are not caused by the processor's acts or omissions.

(d) Except as specifically stated in this clause above and to the extent permitted by GDPR, the liability of processor and controller are as defined in the TOS.

Section III – Final Provisions

Clause 10 – Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may

instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

(e) 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.

(f) If any provision of this DPA is held invalid or otherwise unenforceable, such provision shall be deemed to be severed from the DPA and the enforceability of the remaining provisions shall not be impaired thereby.

Annex I – List of parties

Controller

Name, Address, Contact Details: As set out in any applicable Order Form

Processor

Name: Arnold Media Limited t/a NetRefer

Address: Quantum Place, Triq ix-Xatt, Ta'Xbiex, Gzira, GZR 1020, Malta

Email: dpo@netrefer.com

Tel: +356 2767 3337

Signature and accession date: The Parties agree that execution of the Order Form by the controller and the processor shall constitute execution of these Clauses by both parties as of the Effective Date specified in the Order Form.

Annex II – Description of the processing

Categories of data subjects whose personal data is processed

(i) Prospects, clients, end-users, business partners, suppliers and vendors of NetRefer;

(ii) Employees or contact persons of NetRefer's prospects, clients, end-users, business partners, suppliers and vendors;

(iii) Controller's users / affiliates authorised to use the Service.

Categories of personal data processed

General Personal Data

(i) Device Data (IP, UserAgentString)

(ii) User Data

a. ID, Username, First Name, Last Name, Title, Date of Birth
b. Email address
c. Mobile Number, Telephone Number
d. Skype, Messenger
e. Address, City, Postal Code, Country
f. Passwords

(iii) Payments (IBAN)

Sensitive Data

(iv) Gender - We may receive the Gender with the player Data Transfer.

Nature of the processing

NetRefer will process personal data as necessary to perform the Service pursuant to the Agreement and as further instructed by the controller in its use of the Service.

Purpose(s) for which the personal data is processed on behalf of the controller

NetRefer will process personal data as necessary to perform the Service pursuant to the Agreement and as further instructed by the controller in its use of the Service.

Duration of the processing

NetRefer will process personal data for the duration of the Agreement, unless a longer period is required by applicable laws and regulations. NetRefer shall return the controller's data by enabling the controller to export its data as set forth in the Agreement, and shall anonymise the data or, at the controller's request, delete the data.

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

Data Types	Grounds for Processing	Duration
Affiliate sign up data	Account management and providing access to the Affiliate Management System.	Duration of the Agreement, unless otherwise required by applicable laws.
Affiliate Managers sign up data	Account Management and providing access to the Administration interface of the Performance Marketing Platform.	
Client's Player Registration data	Used to associate the player with the affiliate and verify the acquisition of the player 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.	Duration of the Agreement, unless otherwise required by applicable laws.

Annex III – Technical measures including technical and organisational measures to ensure the security of the data

Security layers and methodologies applied at infrastructure layer:

Network Edge Traffic Monitoring & Mitigation

Simulated & Vetted through Penetration Testing

- **DDoS Simulation Tests**
  A DDoS (Distributed Denial of Service) simulation test is a proactive security measure used to assess NetRefer's readiness to withstand and mitigate DDoS attacks.
- **Penetration Testing**
  Penetration Testing is a security assessment conducted by cybersecurity professionals to evaluate the security of the system, network, or application. During a Pen Test, authorized simulated attacks are performed to identify vulnerabilities that malicious hackers could exploit. The objective is to uncover weaknesses in the system's defences and provide recommendations for improving security measures to protect against real-world threats.
- **Rate Limiting Capabilities**
  Rate limiting capabilities are control measures that help prevent abuse, protect against attacks, and ensure fair usage of resources. When a user exceeds the defined limits, the system may restrict further access or take other actions to maintain stability and security.
- **System Updates**
  System updates refer to the process of installing patches, fixes, or upgrades to software, operating systems, or firmware to improve functionality, enhance security, or address known issues. These updates are released periodically by software vendors or device manufacturers to keep systems up-to-date and protected against emerging threats and vulnerabilities. System updates can include bug fixes, performance improvements, new features, and security enhancements, and they are essential for maintaining the stability, reliability, and security.
- **Multi Factor Authentication**
  MFA adds an extra layer of security beyond just a username and password. This significantly reduces the risk of unauthorized access, as it becomes much harder for attackers to compromise accounts through methods like phishing, brute force attacks, or stolen credentials.
- **Virtual Private Networks**
  VPNs create secure, encrypted connections over the internet, allowing remote users to access a private network as if they were physically present in the same location. VPNs authenticate users and encrypt data to ensure secure remote access.

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
- Change Log
- Authorized Approval of any changes or maintenances

Remote Access Methods

- L2TP/IPSec tunnel VPN protocol
- Data Encrypted in transit
- Access Log
- Change Log
- Management Approval

Systems Security Access Controls

- Managed Azure Active Directory Services (Internal Access)
- 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
- 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 (Internal)
- External Threats to the site
- Physical Intrusion (Internal)

Business Continuity Plan

- High Availability Approach
- Testing of Ad serving application
- Offsite backups of application binary files / configs / media files / scripts
- Multiple ISP providers
- Recovery Time Objective 30 minutes
- Recovery Point Objective last 6 minutes

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).

Security processes at an operational layer

- 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 third 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 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.

Annex IV – List of approved sub-processors

Processing of Personal Data

Personal data may be shared with one or more of the following sub-processors:

Name	Website	Description
Akamai Technologies (GlobalDots) Microsoft Azure Front Door	https://www.akamai.com/ htttps://www.microsoft.com	Edge Security (Web Application Firewall + DDoS)
Microsoft Azure	htttps://www.microsoft.com	Provider for a range of cloud computing services
Atlassian	https://www.atlassian.com/	Provider of Jira Software, used for provisioning customer support
Databricks	www.databricks.com	Provider of data platform
Microsoft Defender	https://www.microsoft.com/en-us/security/business/microsoft-defender	Email Security with deep AI integration with Office 365 Infrastructure threat prevention, detection, and response
Google Analytics	https://support.google.com/?hl=en-GB	User Flow Tracking within Admin/Affiliate platforms
IP2Location	https://www.ip2location.com/	Geographical identification by IP Address
Mailchimp	https://mailchimp.com/	Email marketing
Xero	https://www.xero.com/	Payments infrastructure
Zoho Site24x7	https://www.site24x7.com/	Server and Cloud Monitoring URL Availability and Uptime Monitoring
Hubspot	Hubspot.com	Provider of our customer relationship management platform

For transfers to non-EU controllers, the following will also apply:

STANDARD CONTRACTUAL CLAUSES

Module 4

(International transfer processor to controller – applicable when NetRefer is a processor and Licensee, or Licensee's users, are located outside EU/EEA)

1. 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 - Module One: Clause 8.5 (e) and Clause 8.9(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);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(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.

2. 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 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of Processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and 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 of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and 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 data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and Compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9 – N/A

Clause 10 – Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

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.

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 – N/A

3. 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.

4. 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 collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. 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 a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Malta.

Clause 18 – Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of Malta.

Appendix

Annex I

A. List of parties

Data Importer (Client/Licensee)

Name, Address, Contact Details: As set out in any applicable Order Form

Role: Controller

Data Exporter (NetRefer)

Name: Arnold Media Limited t/a NetRefer

Address: Quantum Place, Triq ix-Xatt, Ta'Xbiex, Gzira, GZR 1020, Malta

Email: dpo@netrefer.com

Tel: +356 2767 3337

Role: Processor

Signature and accession date: The Parties agree that execution of the Order Form by the controller and the processor shall constitute execution of these Clauses by both parties as of the Effective Date specified in the Order Form.

B. Description of the transfer

Categories of data subjects whose personal data is transferred

(i) Prospects, clients, end-users, business partners, suppliers and vendors of NetRefer;

(ii) Employees or contact persons of NetRefer's prospects, clients, end-users, business partners, suppliers and vendors;

(iii) Clients' users / affiliates authorised to use the Service.

Categories of personal data transferred

General Personal Data

(i) Device Data (IP, UserAgentString)

(ii) User Data
   a. ID, Username, First Name, Last Name, Title, Date of Birth
   b. Email address
   c. Mobile Number, Telephone Number
   d. Skype, Messenger
   e. Address, City, Postal Code, Country
   f. Passwords

(iii) Payments (IBAN)

Sensitive Data

(iv) Gender - We may receive the Gender with the player Data Transfer.

Frequency of the transfer

Personal data may be continuously transferred throughout the term of the Agreement.

Nature of the processing

NetRefer will process personal data as necessary to perform the Service pursuant to the Agreement and as further instructed by the Client in its use of the Service.

Purpose(s) of the data transfer and further processing

NetRefer will process personal data as necessary to perform the Service pursuant to the Agreement and as further instructed by the Client in its use of the Service.

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

NetRefer will retain personal data for the duration of the Agreement, unless otherwise specified in the Agreement or a longer retention period is required by applicable laws and regulations. NetRefer shall return the Client's data by enabling the Client to export its data as set forth in the Agreement, and shall anonymise the data or, at the Client's request, delete the data.

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

Data Types	Grounds for Processing	Duration
Affiliate sign up data	Account management and providing access to the Affiliate Management System.	Duration of the Agreement, unless otherwise required by applicable laws.
Affiliate Managers sign up data	Account Management and providing access to the Administration interface of the Performance Marketing Platform.	
Client's Player Registration data	Used to associate the player with the affiliate and verify the acquisition of the player 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 Client's instructions, and affecting system and infrastructure maintenance, software updates and upgrades.	Duration of the Agreement, unless otherwise required by applicable laws.

----------END ----------