# Data Processing Agreement

*Last Modified: 25th May 2018*

*Version 2.2*

***INTRODUCTION***

This NetRefer Data Processing Agreement ("**DPA**") 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.

In all cases NetRefer ("**Processor**"), or a third party acting on behalf of Processor, acts as the Processor of Personal Data and you ("**Controller**"), or any Joint Controller (defined below) remain Controller of Personal Data as per the Data Protection Laws. The term of this DPA shall follow the term of the TOS. Terms not otherwise defined herein shall have the meaning as set forth in the TOS.

***THIS DPA INCLUDES:***

(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) List of Sub-Processors, attached hereto as Appendix D.

(v) Processing Activities, attached hereto as Appendix E.

(vi) Data Retention Policy, attached hereto as Appendix F.

(vii) Contacts and details of the Data Processing Officer, attached hereto as Appendix G.

## 1. **Definitions**

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

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means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR, and all other applicable laws and regulations relating to the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

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

**"Joint Controller"** means where two or more Controllers jointly determine the purposes and means of Processing, they shall be joint controllers as per Article 26 (1) of the GDPR;

"**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;

"**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 data over a network, and against all other unlawful forms of processing.

## 2. **Scope and Responsibility**

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.

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.

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.

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.

## 3. **Obligations of Processor**

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.

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 Processed are Processed solely in accordance with the Processing activities stipulated in Appendix E attached hereto;

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

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.

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.

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, attached hereto as Appendix F.

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.

The Processor shall promptly notify the Controller about:

(i) 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

(ii) any accidental or unauthorised access; and

(iii) 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.

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

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.

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.

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

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

## 4. **Obligations of Controller**

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.

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.

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 data and retain for a period of 2 years for statistical purposes.

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.

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

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.

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.

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.

The Joint Controllers shall in a transparent manner determine their respective responsibilities for compliance with the obligations under GDPR by means of an arrangement between them which shall duly reflect the respective roles and relationships of the Joint Controllers vis-à-vis the Data Subjects.

The essence of the arrangement, together with details of the legal or DPO contact persons of the Joint Controllers and of the Data Subjects, shall be made available also to the Processor to enable the Processor to meet its obligations to the specific Controller.

The Controller shall ensure that any obligations under this DPA are also reflected in the aforesaid arrangement, irrespective of which of the Joint Controllers has entered into this DPA.

## 5. **Enquiries by Data Subjects to Controller**

Where Controller, based upon applicable data protection law, 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:

(i) Controller has instructed Processor in writing to do so, and
(ii) Controller reimburses Processor for the costs arising from this assistance.

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.

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

## 6. **Sub-Processors**

Processor shall be entitled to subcontract Processor's obligations for the fulfilment of the Processing services to third parties only with Controller's written consent.

Controller consents to Processor's subcontracting to the Processor's affiliated companies and third parties that are listed in Appendix D.

If the Processor intends to instruct Sub-Processors other than those listed in Appendix D, 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 must give the Controller the possibility to object against the instruction of the Sub-Processor 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, either party may terminate the Agreement by providing written notice to the other party.

Where Processor engages Sub-Processors, Processor shall be obliged to pass on Processor's contractual obligations hereunder to such Sub-Processors. This shall apply in particular, but shall not be limited to, the contractual requirements for confidentiality, data protection and data security stipulated between the parties of the Agreement.

Where a Sub-Processor is used, the Controller must be granted the right to monitor and inspect the Sub-Processor in accordance with this DPA, including the right to conduct its own due diligence of the Sub-Processor.

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

## 7. **Transfer of Personal Data**

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.

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.

## 8. **Duties to Inform, Additional Terms**

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.

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.

## 9. **Returning or Destruction of Personal Data**

Upon termination of this Data Processing Agreement, upon the Controller’s written request, or upon fulfilment of all purposes agreed in the context of the Products whereby no further processing is required, the Processor shall, at the discretion of the Controller, either delete, destroy or return all Personal Data to the Controller and destroy or return any existing copies.

The Processor shall notify all 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 shall either destroy the Personal Data or return the Personal Data to the Controller, at the discretion of the Controller.

## 10. **Audit Obligations**

The Processor shall endeavour to carry out a yearly audit of compliance from a security and data protection perspective, the results of which are to be shared with the Controller upon request.

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

(i) 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.

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

(iii) All costs related to auditors’ fees are to be borne by the Controller.

(iv) 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.

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.

## 11. **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*** – PrevenTier & Incapsula

*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.

## 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.
- All 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.
- NetRefer has a security board made up of representatives from each department to identify, record and rectify any risks and threats.
- Processes are in place to ensure security testing is carried out internally per release as well as annually 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 monthly 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 processes to ensure adherence to the Data Retention Policy specified in Appendix F.

## Appendix D: List of Sub-Processors

***Sub-Processors***

- Microsoft
- Rackspace
- Incapsula
- Pingdom
- Site24x7
- Application Insights
- Hotjar

Systems provided by NetRefer may allow for integrations with other 3rd party Processors such as those listed below.

***3rd Party Integration Processors***

- HasOffers
- NetTeller
- MoneyBookers
- AppsFlyers
- BannerFlow
- NCCGroup Escrow Services

Note that in the case of such integrations, data is transferred to additional 3rd Party Integration Processors only if the related integration or service has been purchased from NetRefer.

In such cases, a contract is required between the 3rd Party Integration Processor and the Controller to govern the data processing from the 3rd Party Integration Processor's end as they would be considered direct Processors of the Controller and not as Sub-Processors of the Processor under this Agreement.

## Appendix E: Processing Activities

| Processing Activity | Data Types | Grounds for Processing |
|---|---|---|
| | | |
| Collection & Storage | Affiliate sign up data | Account management and providing access to the Affiliate Management System. |
| Collection & Storage | Affiliate Managers sign up data | Account Management and providing access to the Administration interface of the Performance Marketing Platform. |
| Collection, Storage & Processing | 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. |
| Collection, Storage & Processing | Transactional Activity | Processed and aggregated for the purpose of calculating the affiliate rewards. |
| Collection, Storage & Processing | Affiliate payment information | Processed for the purpose of generating the payment files for affiliates. |
| Tracking, Collection, Storage & Processing | Marketing media views and clicks | ▪ Processed for the purpose of<br>▪ tracking, media, campaign and affiliate performance.<br>▪ Linking a customer to an affiliate<br>▪ Rewarding affiliates |
| Processing | Affiliate, Customer, Views, Clicks and rewards | Generation of statistics, performance metrics and KPIs for<br>▪ Affiliate management<br>▪ Affiliate performance<br>▪ Rewarding<br>▪ Financial reporting<br>▪ Benchmarking |
| **Processing** | All data within the systems | For the purposes of executing instructions of the Controller. |
| **Processing** | All data within the systems | For the purpose of affecting system maintenance, updates or upgrades of the software as well as the infrastructure. |
| **Collection, storage** | Controller’s Employee basic data | For the purpose of providing credentials to internal NetRefer support tools and mechanisms. |

## Appendix F: Data Retention Policy

***Introduction & Scope***

A data retention policy, or records retention policy, is an organization's established protocol for retaining information for operational or regulatory compliance needs.

The data retention period refers to the length of time that a type of data will be stored and available. This includes via backup media and currently accessible methods.

The scope of the below policy is limited to electronic data in relation to the client's systems and communications between NetRefer's client and NetRefer and covers both Personal Data and regular data.

NetRefer collects the minimum of personal or sensitive data required for the provision of services under the Agreement. Further details can be found in Appendix E: Processing Activities.

In lieu of complete erasure when personal or sensitive data types are involved NetRefer uses aggregation and obfuscation to preserve both the anonymity of the Data Subject as well as the integrity of the data within the systems.

The retention and archival periods defined below are based on the legitimate interest of NetRefer as well as legal obligations. As such, should the relevant interest, legislation, laws or regulation be updated or modified, the retention and archival periods listed below shall be adjusted accordingly for the purpose of compliance.

***Record Retention Schedule***

<table>
<tr><td colspan="4"><b>RECORD RETENTION SCHEDULE</b></td></tr>
<tr><th>Data Type/System</th><th>Retention Period</th><th>Archival Period</th><th>Description</th></tr>
<tr><td colspan="4"><b>General electronic communications</b></td></tr>
<tr><th>Data Type/System</th><th>Retention Period</th><th>Archival Period</th><th>Description</th></tr>
<tr><td>E-Mail</td><td>2 years</td><td>10 years</td><td>Falls under general communication<br>After 10 years on archive, emails will be automatically and permanently deleted.</td></tr>
</table>

| | | | |
|---|---|---|---|
| JIRA Tickets for decommissioned clients | 1 years | 6 years | Retention periods are in accordance with local laws as such data qualifies as general business correspondence under Maltese company laws. |
| JIRA Tickets for live/active clients | Lifetime* | | *Until end of life (decommissioning request) |

## NetRefer Systems & Services

**Performance Marketing Platform**

| **Data Type/System** | **Retention Period** | **Archival Period** | **Description** |
|---|---|---|---|
| Client Registrations & Activity files* | 3 months | rolling 24 months | Referring to the physical files sent over by clients to process the data in the Performance Marketing Platform.<br>*For active clients. Values are of a discretionary nature, taking into consideration that the activity and registration files translate into rewards for affiliates which in turn generate payment and that NetRefer is not the one true source of this data. |
| Client Payment files | 3 years | 6 years* | Referring to the physical files generated by the NetRefer System used by the client to process any payments.<br>Values are discretionary taking into consideration the legal indication that any financial records are to be kept for 6 years. However, these can be kept in archive to be retrieved upon request. Directly accessible 3 years, determined following client feedback.<br>**A further 3 years beyond the directly accessible period.* |
| Views & Clicks | 90 days (raw)<br>3 years (aggregated) | Lifetime* (aggregated) | *Until end of life (decommissioning request) |

| | | | |
|---|---|---|---|
| Database for live/active clients (as is) | 3 years | Unlimited* | *Until end of life (decommissioning request) |
| Database for decommissioned clients | 0 months | 2 years | |
| Physical log files for active clients | 90 days – 6 months* | 1 – 3 years* | Such as IIS logs, event viewer, intrusion detention system logs.<br>*Depending on the type of logs |
| Physical log files for decommissioned clients | 0 months | 90 days | |
| Backups for live/active clients | 3 days | 4 weeks | Backups are taken daily, archival and deletion are on a rolling base frequency. |
| Backups for decommissioned clients | 0 days | 4 weeks | |
| **Performance Marketing Intelligence System (PMI)** | | | |
| **Data Type/System** | **Retention Period** | **Archival Period** | **Description** |
| Live clients | 3 years | unlimited* | *Until end of life (decommissioning request) |
| Decommissioned Clients | 0 months | 2 years | Aggregated & obfuscated for statistical purposes, as long as the client has not requested complete deletion upon termination. |

## Appendix G: Contacts of the Data Processing Officer

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's Data Protection officer at 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.