ANNEX A19 – DATA PROCESSING AGREEMENT

ANNEX A19 – DATA PROCESSING AGREEMENT

The following terms address the Customer's compliance obligations under applicable Data Protection Law and is applicable only if and to the extent that applicable Data Protection Law applies to the processing of any personal data by BMIT Limited, its affiliates, successors and assigns ("BMIT" or the "Service Provider") to its customers ("Customer") in relation to the Services provided by BMIT to the Customer.

These terms are ancillary to the Master Agreement. Upon expiry or termination of the Master Agreement, these Terms and Conditions shall be deemed automatically terminated.

A19-1. **Additional Definitions.** For the purposes of this Annex, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

(a) ***"data protection legislation"*** shall refer to the legislation on the protection of personal data applicable in Malta and, in particular, to the Data Protection Act (Cap. 586 of the Laws of Malta); and the EU General Data Protection Regulation (Reg. 2016/679) which may in particular also be referred to as the 'GDPR';

(b) ***"personal data"*** shall have the same meaning as ascribed in applicable data protection legislation and shall extend and apply to any personal data held by legal and/or natural persons;

(c) ***"data subject"***, ***"processing"***, and ***"data breach"*** shall have the same meaning as ascribed in applicable data protection legislation;

(d) ***"IT system"*** means an information technology system which is the subject of the Services or to which the Services relate;

(e) ***"end-users"*** means the Customer's own customers and affiliates whose personal data is processed by BMIT through the provision to, or use by, the Customer of the Services.

A19-2. **Data Processing and Protection.** With respect to any personal data that the Customer may have access to and store or process on its IT system, the Parties agree that:

A19-2.1. The Customer may be either (a) a Controller of Customer Personal Data, or (b) a Processor when it Processes Customer Personal Data on behalf of its end-users.

A19-2.2. BMIT is a Processor where the Customer is a Controller or Processor, or a sub-processor when Customer is acting as a Processor on behalf of its end-users;

A19-2.3. The purpose of any Processing that is performed by BMIT is to provide Services to Customer under the Agreement and the detection, prevention and resolution of technical issues as provided for in the applicable Agreement and any purposes compatible therewith, and the subject matter of such Processing is BMIT's provision and Customer's use of the Services and the detection, prevention and resolution of technical issues as provided for in the applicable Agreement.

A19-2.4. BMIT will Process Personal Data only: (a) in a manner consistent with documented instructions from Customer, which will include Processing (i) to provide the Services, (ii) as authorized or permitted under the Principal Agreement, and (iii) consistent with other reasonable instructions of Customer; and (b) as required by applicable law, provided that BMIT will inform the Customer (unless prohibited by such applicable law or in the case of urgency) of the applicable legal requirement before Processing pursuant to such applicable law. In the circumstances were either as a result of a legal obligation, lawful request or legitimate criteria BMIT are obliged to take a decision on the processing of the personal data, Controller obligations will apply in line with applicable legislation.

A19-2.5. The type of Personal Data Processed is any Personal Data provided or made available to BMIT by or on behalf of Customer through the use or provision of the Services.

A19-2.6. The categories of Data Subjects are those whose Personal Data are provided or made available to BMIT by or on behalf of Customer through the use or provision of the Services, including staff, Customers, partners of Customer or End-users and any End- users who are individuals.

A19-3. **Customer Obligations**. The Customer will not instruct BMIT to perform any Processing of Personal Data that violates any Data Protection or Privacy Law. The Customer represents and warrants that any Processing of Personal Data by BMIT performed in accordance with the Principal Agreement does not and will not violate any Data Protection Law. BMIT may suspend Processing based upon any instructions given by the Customer that BMIT reasonably suspects violate Data Protection Law. The Customer will be solely liable for the legality of Processing, and, subject to the cooperation of BMIT as specified in this Addendum, for safeguarding the rights of Data Subjects. The Customer will promptly notify BMIT about any faults or irregularities that it discovers in any Processing by BMIT.

In respect of data which the Customer receives, stores, or transmits on or using its IT System, (i) in addition to Customer's obligations stated in the Agreement, the Customer is responsible for the integrity, security, maintenance and appropriate protection of Customer Personal Data, and ensuring its compliance with any privacy laws and regulations applicable to its own Processing of the Customer Personal Data and its use of the Services, including Applicable Data Protection Law; (ii) Customer controls how Customer Personal Data is stored, classified, exchanged, or otherwise Processed when using the Services; (iii) Customer may select the territory in which it stores and Processes Customer Personal Data and may implement and maintain, or purchase supplementary services from BMIT, in order to put in place those technical and organizational security measures appropriate to the nature and volume of Customer Personal Data that Customer Processes using the Service.

A19-4. **Security & Confidentiality Obligations**. BMIT will protect Personal Data in accordance with requirements under Data Protection Law, including by implementing appropriate technical and organizational measures designed to protect Personal Data against any Data Breach that will meet or exceed the requirements specified in BMIT's Information and Security Policy. BMIT will ensure that persons authorized by BMIT to Process any Personal Data are subject to appropriate confidentiality obligations.

A19-5. **Return or Disposal**. At the choice of the Customer, BMIT will delete or return (or will, if technically, operationally and legally possible, enable the Customer via the Services to delete or retrieve) all Personal Data after the end of the provision of Services unless any applicable legal obligation or right requires the storage of such Personal Data by BMIT.

A19-6. **Data Subject's Rights Assistance**. Taking into account the nature of the Processing of Personal Data by BMIT under the Agreement, BMIT will provide reasonable assistance to the Customer by appropriate technical and organizational measures, insofar as possible and as necessary, for the fulfilment of the Customer obligations to respond to requests for exercising Data Subject's rights under Chapter III of the GDPR with respect to Personal Data solely to the extent that the Customer does not have the ability to address such Data Subject request without such assistance.

A19-7. **Security Assistance**. To assist the Customer in its efforts to ensure compliance with the security requirements under Article 32 of the GDPR, BMIT has made available to the Customer its Information and Security Policy in sub-annex A19a included with this annex.

A19-8. **Data Protection Impact Assessment Assistance**. The Customer acknowledges that BMIT has no knowledge of the Customer Personal Data received, stored, or transmitted on or using its IT System. Taking into account the nature of BMIT's Processing of Personal Data and the information available to BMIT, BMIT will provide reasonable assistance to the Customer, at Customer's expense, as required for the Customer to comply with its obligations under Articles 35 and 36 of the GDPR in connection with BMIT's Processing of Personal Data under the Principal Agreement.

A19-9. **Personal Data Breach Notice and Assistance**. BMIT will notify the Customer without undue delay after becoming aware of a Personal Data Breach. Taking into account the nature of Processing and the information available to BMIT, BMIT will provide reasonable assistance to the Customer as may be necessary for the Customer to satisfy any notification obligations required under Articles 33 or 34 of the GDPR related to any Personal Data Breach.

A19-10. **Audits**. BMIT will allow for and contribute to audits, including inspections and as required or permitted under the Standard Contractual Clauses, conducted by the Customer or another auditor mandated by the Customer that is reasonably acceptable to BMIT in accordance with the terms of this clause 4 throughout the validity of the Principal Agreement and for a further period of one year. Any such audit must occur during BMIT's normal business hours and will be permitted only to the extent required for the Customer to assess BMIT's compliance with this Addendum.

In connection with any such audit, the Customer will ensure that the auditor will: (a) review any information on BMIT's premises; (b) observe reasonable on-site access and other restrictions reasonably imposed by BMIT; (c) comply with BMIT's on-site policies and procedures, and (d) not unreasonably interfere with BMIT's business activities. BMIT reserves the right to restrict or suspend any audit in the event of any breach of the conditions specified in this clause. The Customer auditor will not be entitled to access information subject to third-party confidentiality obligations. The Customer will provide written communication of any audit findings to BMIT, and the results of the audit will be the confidential information of BMIT.

Insofar as this is possible and allowed, the Customer will provide no less than fifteen (15) days' advance notice of its request for any such audit, and will cooperate in good faith with BMIT to schedule any such audit on a mutually agreed upon date and time (such agreement not to be unreasonably withheld by either party).

A19-11. **Sub-processors**. The Customer authorizes BMIT to use BMIT's affiliates and third-party Sub-processors to Process Personal Data in connection with the provision of Services to the Customer (hereinafter 'Sub-processor'). BMIT will inform the Customer in writing of any intended changes concerning the addition or replacement of its Sub-processors, and provide the Customer with the opportunity to object to such changes. If the Customer objects to any Sub-processor, BMIT may terminate the Principal Agreement immediately upon notice to Customer without liability to either party. BMIT will impose data protection obligations upon any Sub-processor that are no less protective than those included in this Addendum.

A19-12. **Data Transfers**. BMIT is located within the EU. However, to the extent that Personal Data may be transferred to, stored and/or processed in any country in which BMIT, its affiliates or its Sub-processors maintain facilities outside of the EU, the European Economic Area or Switzerland that has not received a binding adequacy decision in accordance with applicable Data Protection Legislation (hereinafter a 'Third Country'), BMIT will conduct such transfer: (a) pursuant to the EU Standard Contractual Clauses which may be applicable from time to time and which, at the time of signature, are available at http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087; or (b) any other data transfer mechanism permitted under applicable Data Protection Legislation.

A19-13. **Customer Affiliates**. To the extent that BMIT may process Personal Data on behalf of the Customer affiliates in accordance with the Principal Agreement, the Customer enters into this Addendum on behalf of itself and as agent for its affiliates, and any references to the Customer under this Addendum shall include the Customer and its affiliates, provided however that the Customer shall be the sole entity which may enforce this Addendum on its own behalf and on behalf of its affiliates.

Annex A19b – BMIT Information & Security Policy

1. Overview

BMIT, hereunder referred to as the ***"Company"***, understands the importance of data security and makes every effort to ensure that customer data held on its systems or on any systems which are hosted within the company's data centres are fully protected.

The Company recognizes that the confidentiality, integrity and availability of information and data created, maintained and hosted by the Company and its customer's is vital to the success of the business.

The Company's management view these as primary responsibilities and fundamental to best business practice and as such has adopted the Information Security Management System Standard BS ISO/IEC 27001:2013 and PCI DSS as its means to manage and meet the following objectives:

1. Comply with all applicable laws, regulations and contractual obligations including the Data Protection Act (GDPR).
2. Implement continual improvement initiatives, including risk assessment and treatment strategies, while making the best use of its management resources to meet and improve information security system's requirements.
3. Communicate its Information Security objectives and its performance in achieving these objectives, throughout the Company and to interested parties.
4. Adhere to the Information Security Management System (ISMS) comprising of a security manual and procedures that provides direction and guidance on information security matters relating to employees, customers, suppliers and interested parties who come into contact with the Company's work.
5. Work closely with their customers, business partners and suppliers in seeking to establish Information Security Standards.
6. Adopt a forward-looking view on future business decisions, including the continual review of risk evaluation criteria, which may have an impact on Information Security.
7. Train all members of staff in their needs and responsibilities for Information Security Management.
8. Constantly strive to meet, its customers and staff expectations.
9. Information Security shall be considered in job descriptions and when setting staff objectives where applicable.
10. Appropriate Information Security training and awareness shall be provided to all staff to ensure principals and practices are embedded in the company culture.

2. Purpose

The purpose of this document is to provide information about the procedures Company maintains to ensure the security of its customers' data, software and systems.

This document will cover the following areas:

1. Customer Authentication
2. Physical Security
3. Access Control
4. Network Security
5. Software Security
6. Media Handling

7. Auditing and Monitoring
8. Contingency Planning
9. Recruitment and Training

This policy applies to all Company employees or any other individual or supplier working for Company. Company management team are responsible for ensuring full compliance with this policy.

Unless written permission is obtained by the ISMS chairperson, no part of this policy and other relevant policies can be ignored or bypassed. It is the responsibility of all staff members to report any such incidents in a timely fashion. It is the responsibility of the ISMS to review such incidents and identify the correct course of action.

The CTO was appointed by the management to provide an annual executive summary of the ISMS.

3. Data Protection

The Company is committed to complying with data protection legislation as documented in AD-POL-2018-003 - General Data Protection Policy and good practice including:

- processing personal information only where this is strictly necessary for legitimate organisational purposes;
- collecting only the minimum personal information required for these purposes and not processing excessive personal information;
- providing clear information to individuals about how their personal information will be used and by whom;
- only processing relevant and adequate personal information;
- processing personal information fairly and lawfully;
- maintaining an inventory of the categories of personal information processed by the Company;
- keeping personal information accurate and, where necessary, up to date;
- retaining personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate organisational purposes;
- respecting individuals' rights in relation to their personal information, including their right of subject access;
- keeping all personal information secure;
- only transferring personal information outside the EU in circumstances where it can be adequately protected;
- the application of the various exemptions allowable by data protection legislation.

4. Customer Authentication

Any support requests sent to the Company from Customers, for information about their service or to request assistance must be validated to ensure they are who they say they are. This will reduce the risk of loss of confidentiality and data breaches.

In the event that an unauthorized individual contacts the Company:

- The procedures and policies outlining authorization requests, including a blank authorization form if onetime only, are provided to the client who is advised to have these filled by an authorised contact;

- No requests are entertained from the unauthorized client;
- An e-mail is sent to the Authorised official and/or contract signatory with the name and request of the individual requesting access.

5. Physical Security

The Company's data centre facilities are diversely located in Handaq and Smart City Malta and connected by secure, resilient high speed back-up links. Both of our data centres have the following physical security features in place to protect both equipment and customer data.

All racks within the data centres are equipped with fully lockable doors which only authorised engineers have access to. Proximity door locks are fitted on all internal and external doors and extensive CCTV monitoring systems are installed on all internal and external walls.

CCTV monitoring systems include motion detection features that trigger CCTV recording in the event of any movement both inside and outside of the data centres (within the cameras' range).

Company operates Uninterruptible Power Supply (UPS) systems and diesel generators on all of it sites to ensure that services remain available in the event of a power failure.

Full access control systems are in place that only allows authorized employees to secure areas. No other employees, customers or third parties are authorised to access these areas unless accompanied by an authorised engineer.

Any visitor access is strictly as per AD-PRC-2011-002 - Authorisation Clearance. All visitors are required to provide one week's prior written notice of their visit and produce photo ID upon arrival at the data centre. The visitor's log sheets are kept indefinitely.

All Company staff are required to carry their site access and identification card with them at all times and access is restricted to authorised areas only. The Company's management team reserves the right to refuse access to anyone without a site access card.

6. Access Control

Access to Company's internal systems, data floors, hosting platform and customer infrastructure is permitted for authorised personnel only. All persons must be positively identified by providing a secure User ID and password before being given access to system resources.

Access rights (privileges) to system access are given only to the users who need to access the system. The access rights given to each user are recorded in the Access Declaration Form, document number AD-FOR-2011-019.

When remote access is required, a VPN connection must be used. Attempts to circumvent using the VPN connection for remote access are considered as a serious breach of security.
Users are only granted a logon by the explicit approval of the C.T.O. and corresponding form AD- FOR-2011-019 must be filled accordingly. Usernames and passwords for VPN users must follow the password policy. The VPN must, at a minimum have:

- two factors of authentication;
- Encryption;
- Be unique to each user;

Only Company's Core Engineers have full access to the hosted platforms, each engineer having their own individual login for optimum security. Authorised support staff have limited access to hosted services in order to provide technical support to customers.

7. General Security and Passwords

Any computer terminal with access to Company data must follow Company's security policies. The user is responsible for the security of any computer terminal being used. Each unattended terminal needs to be locked, in order to prevent unauthorised users accessing the system.

Users need to select secure passwords. Passwords should not be dictionary words and should not have personal identifiable and guessable information. Passwords must not be stored or transmitted in plain text. Passwords should not be lent. Company reserves the right to enforce the password selection process and to audit such at intervals.

The company has a clear desk and clear screen policy. It is expected that all confidential information in hardcopy or electronic form is secure, particularly at the end of the day and when expected to be away for an extended period of time.

8. Acceptable Use

8.1. Internet Files and Software

Employees must not download or accept any software that is not required for business purposes. Employees must screen all files downloaded from the Internet with virus detection software.

Employees must not make illegal copies of copyrighted software. All software used on employees' computers within the firm must be a licensed copy and must adhere to the software owner's copyright conditions.

8.2. Monitoring of Internet Use

The Company reserves the right to monitor and log all connections between their networks and the Internet. These logs include the user's name and those of the sites accessed. Such activity will be kept as per the retention policy.

8.3. Blocking of Internet Sites

The Company reserves the right to block access to any Internet site or resource deemed inappropriate.

8.4. Access Rights

Users who do not have administrative access must NOT try to circumvent such enforcements. If users are found to have breached such security, disciplinary action might be enforced. This includes:

- Making changes to circumvent security software or other restrictions in place;
- Using systems that are not authorised by the Company to store and/or process data;
- The use of portable applications that are against policies;
- Making systems unavailable for one or more users through the use of unauthorised network devices;
- Attempting to impersonate other users.

9. Network Security

The network design is intended to deliver high performance and reliability to meet the needs of the operations whilst providing a high degree of access controls and range of privilege restrictions. The configuration of network impacts directly on its performance and affects its stability and information security.

The network design takes into consideration that:

- Poor network stability can threaten operations;
- Inadequate control over access to network can jeopardize the confidentiality and integrity of data;

- Slow or inadequate system response times impede the processing.

9.1. Managing the Network

The network is managed by the Core Team. Changes must be analysed for any potential security risk introduction.

9.2. Accessing the Network Remotely

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. The needs for remote access are to be clearly defined before it is granted. Users which require remote access will often be connecting through public unsecure networks. This increases the threat of unauthorized access - therefore all individuals with remote access need to be advised of the risks and follow the procedure which is put in place governing how they connect to the intranet.

9.3. Defending Network Information from Malicious Attack

All system hardware, operating and application software, the networks and communication systems are safeguarded at all times from physical access or network intrusion. All physical hardware is kept within designated rooms and/or cabinets which can only be accessed by the technical staff. The technical staff is also responsible for ensuring that all network access points are secured. Unused ports are to be kept in disabled status on the network device. Non-IP authorized systems are denied access to critical systems.

Network cabling is also segregated from Power cabling to ensure no interference is experienced. Special cable trays exist within the designated areas for cable runs to be passed neatly and safely to make sure they are not affected.

Access to designated areas is defined by the user's job requirements and controlled by their card access.

10. Software Security

The Company operates a strict software security policy throughout the organisation to provide increased security across the network. This policy is governed by an IT Code of Conduct and all software loaded onto Company's IT systems must be legally purchased and licensed and access to install programmes is restricted to members of the Core team only.

The Company's Core Engineers are responsible for all software security updates on Company's infrastructure and any application launched on Company's infrastructure must have its suitability verified by Company's Core Department and approved by the CTO prior to rollout

Furthermore, Company employees must ensure that systems are conforming to security policies set up by the company. The employee must NOT in any way tamper or impede with these operations:

- Anti-Malware software is installed, up to date and allowed to perform regular scans;
- The software firewall is enabled and maintained properly;
- Secure methods are used to transfer files;
- Authentication is set up on all systems;
- User is logged out following inactivity periods;
- Understand the features installed are to assist with security and not hinder the user;
- Use a high security level on your Internet browser;
- Never share any details on security.

11. Media Handling

11.1. Media Handling as Classified

Information classification is extremely important as the information handling process is built upon it. The list below identifies the basic handling guidelines for the data as classified. It is noted that identified data assets may be subject to specified handling as listed on Company's ISMS management system.

Data Classification	Public or un-classified	Confidential Internal Use	Confidential Other
Markings	None required	Documents should be marked for Internal Use Only	Documents must be marked as Confidential
Physical and Logical Controls	None required	The author should make sure proper markings are in place. Users are required to ensure information is stored and controlled.	Author is responsible for ensuring information is not available for distribution and is clearly marked. Recipients must not share the information.
Reproduction	Unlimited or as per Copyright	Limited copies may be made only if necessity arises.	Limited copies may be mode under the approval of the original distributor.
Distribution	No restrictions	– Internal unrestricted; – External sealed envelope; – Electronic use encryption for external transmission	– Internal - sealed envelope; – External - sealed envelope and sent by registered mail or hand delivered; – Electronic – encrypted
Disposal	Trash	– Printed media shredded; – Electronic media sent to 2nd Level support for correct archiving or media disposal as per media handling policy.	– Printed media - shredded; – Electronic media - sent to 2nd Level support for correct archiving or media disposal as per media handling policy.

11.2. Disposal of media

The disposal of client's media is the sole responsibility of the client and Company the Company is not responsible for the safe disposal and/or destruction of said media.

Where the media belongs to the Company, the media is archived permanently in secure storage with limited access. Where the need arises for the backup media to be disposed entirely, it must be destroyed through appropriate means and where required, a certificate for the destruction of media is issued accordingly from the responsible parties for the destruction.

Paper media must be shredded. It is often best to shred multiple sheets at the same time to help ensure that the contents cannot be reassembled.

12. Auditing and Monitoring

Having visibility of the activity ongoing on the network infrastructure is crucial to maintain the expected level of service availability, performance and security. All Company Core Networking equipment (switches and routers) must keep an activity log on an external syslog server. Modify access to the syslog server is restricted to the core team.

Every day an automated script checks all the logs on each server and analyses the content. It then emails a report to the core team with any warnings found. If no warnings are found, a report is still sent to advise the green status of the equipment.

All issues are logged by Service Requests and major faults or problems relating to the network are escalated to the Core team and/or CTO accordingly.

13. Contingency Planning

In line with our ISO 27001 certification, Company operates its own disaster recovery procedures. In the event of any security issue being identified, an escalation process is in place whereby engineers are alerted by Service Request. Upon completion of the remedial work and resolution of the fault, the Service Request is closed.

The Company has a continued, ongoing commitment to data security and availability. In addition, Company reserves the right to take all contractual allowable measures in respect of a customer's service if it is believed that the use of the service constitutes a security threat to Company or any other users/customer on Company's infrastructure.

14. Recruitment and Training

All candidates employed by Company are subject to screening. As part of this process, all references are followed up for new employees and security training is included within both the induction training programme and also ongoing.

Company implements an internal IT Code of Conduct that all employees must adhere to so as to ensure security and integrity of software, systems, hardware and data, in line with the requirements of ISO 27001 and PCI DSS. All employees with operational responsibilities are subject to Baseline Personnel Security Standard checks.