Data Processing Agreement

(GDPR and EU Standard Contractual Clauses - May 2018)

This Data Processing Agreement ("DPA"), forms part of the Agreement or Terms of Service between the Customer and AIS Technology Limited ("AIS") and shall be effective on the date Customer signed to accept or the Parties otherwise agreed to this DPA ("Effective Date"). This Data Processing Agreement reflects the Parties' agreement with respect to the terms governing the processing and security of Customer Data under the applicable Agreement. Signing this agreement also infers that the Customer has accepted AIS's Terms of Service and Privacy Policy.

This Data Protection Agreement (hereinafter referred to as the "Agreement") is entered into at the

date _____ by and between _____, (which shall be referred to hereinafter as Customer), with registration number _____with registered office at_____, as duly represented hereon (which shall be referred to hereinafter as the "Customer" or "Data Controller"), and,

AIS Technology Limited which shall be referred to hereinafter as "AIS", with registration number C12537, VAT number MT10294129, a company organised and existing under the laws of Malta with registered office at BLB903, Bulebel Industrial Estate, Zejtun, ZTN3000, Malta, as duly represented hereon (which shall be referred to as the "Data Processor" or "AIS").

Customer and AIS hereinafter collectively referred to as the "Parties" and individually as the "Party".

1. Background

Whereas:

1.1. AIS develops and licences its own software, sells licences for related Third-party software, provides subscriptions for Software-as-a-Service applications (including Spektrum) and provides other related services, including software development, support and maintenance, consulting services and other services in the area of Information Technology, to the Customer collectively known as the Services.

1.2. In providing the Services, AIS may collect, manage or process Personal Data within the meaning of Data Protection regulations.

1.3. The Parties are aware of the EU legislation on data protection, means 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, and repealing Directive 95/46/EC, hereinafter referred to as GDPR.

1.4. The Parties agree to enter into this Data Protection Agreement, hereinafter referred to as DPA, which governs the data protection obligations of the Parties when processing the Customer's Personal Data, and which governs the relationship between the Parties in relation to the processing of Personal Data.

2. Definitions

In this Data Processing Agreement, the following terms shall have the meanings set out below, unless stated otherwise:

2.1. "Affiliate" means any entity controlling, controlled by, or under common control with a party, where "control" is defined as: (a) the ownership of at least fifty percent (50%) of the equity or beneficial interests of the entity; (b) the right to vote for or appoint a majority of the board of directors or other governing body of the entity; or (c) the power to exercise a controlling influence over the management or policies of the entity.

2.2. "Agreement" means AIS's Terms of Service, which govern the provision of the Services to Customer, as such terms may be updated by AIS from time to time.

2.3. “Customer Data” means data submitted, stored, sent or received via the Services by Customer, its Affiliates or End Users.
2.4. “Customer Personal Data” means personal data contained within the Customer Data.
2.5. "Data Controller" means an entity that determines the purposes and means of the processing of Personal Data.
2.6. “Data Incident” means a breach of AIS’s security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by AIS. “Data Incidents” will not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.
2.7. "Data Processor" means an entity that processes Personal Data on behalf of a Data Controller.
2.8. “Data Protection Laws and Regulations” means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.
2.9. “Data Subject” means the identified or identifiable person to whom Personal Data relates.
2.10. “EEA” means the European Economic Area.
2.11. “European Data Protection Legislation” means, as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland).
2.12. “GDPR” means 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, and repealing Directive 95/46/EC.
2.13. “Notification Email Address” means the Account Owner Email Address (by default, email address used to sign up for the AIS account).
2.14. "Personal Data" means any information relating to an identified or identifiable natural person.
2.15. "Processing" has the meaning given to it in the GDPR and "process", "processes" and "processed" shall be interpreted accordingly.
2.16. “Security Documentation” means all documents and information made available by AIS under Section 6.4.1 (Reviews of Security Documentation).
2.17. “Security Measures” has the meaning given in Section 6.1.1 (AIS’s Security Measures).
2.18. “Services” means any product or service provided by AIS to Customer pursuant to the Agreement.
2.19. “Sub-Processors” means third Parties authorized under this Data Processing Agreement to have logical access to and process Customer Data in order to provide parts of the Services and related technical support.
2.20. “Term” means the period from the Effective Date until the end of AIS’s provision of the Services under the applicable Agreement, including, if applicable, any period during which provision of the Services may be suspended and any post-termination period during which AIS may continue providing the Services for transitional purposes.

3. Duration of Data Processing Agreement

3.1. This Data Processing Agreement will take effect on the Effective Date and, notwithstanding expiry of the Term, remain in effect until, and automatically expire upon, deletion of all Customer Data by AIS as described in the Agreement.

4. Processing of Personal Data

4.1. Roles of the Parties: The Parties acknowledge and agree that with regard to the Processing of Customer Personal Data, Customer is the Controller, AIS is the Processor and that AIS will engage Sub-Processors pursuant to the requirements set forth in Section 10 “Sub-Processors” below.
4.2. Customer’s Processing of Personal Data:
4.2.1. The Customer shall, in its use of the Services, Process Customer Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, the

Customer's instructions for the Processing of Customer Personal Data shall comply with Data Protection Laws and Regulations.

4.2.2. The Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which the Customer acquired the Customer's Personal Data.

4.3. AIS's Processing of Personal Data

4.3.1. AIS shall treat the Customer Personal Data as Confidential Information and shall only Process Customer Personal Data on behalf of and in accordance with the Customer's documented instructions. The Customer hereby instructs AIS to process Customer Personal Data for the following purposes:

4.3.1.1. Processing in accordance with the Agreement and in providing related technical support;

4.3.1.2. Processing initiated by Users in their use of the Services; and

4.3.1.3. Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

4.4. Details of the Processing

4.4.1. The Parties acknowledge and agree that the subject matter and details of the processing are described in Appendix 2.

5. Return and Deletion of Customer Data

5.1. AIS shall return Customer Data to Customer and, to the extent allowed by applicable law, delete Customer Data in accordance with the procedures and timeframes specified in the Agreement.

6. Data Security

6.1. AIS's Security Measures, Controls and Assistance

6.1.1. AIS's Security Measures

6.1.1.1. AIS will implement and maintain technical and organisational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 1, Appendix 2 (the "Security Measures") of the Addition. As described in Appendix 1, Appendix 2, the Security Measures include measures to encrypt personal data; to help ensure ongoing confidentiality, integrity, availability and resilience of AIS's systems and services; to help restore timely access to personal data following an incident; and for regular testing of effectiveness. AIS may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

6.1.2. Security Compliance by AIS Staff

6.1.2.1. AIS will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Sub-processors to the extent applicable to their scope of performance, including ensuring that all persons authorized to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6.1.3. AIS's Security Assistance

6.1.3.1. The Customer agrees that AIS will (taking into account the nature of the processing of Customer Personal Data and the information available to AIS) assist Customer in ensuring compliance with any of Customer's obligations in respect of the security of personal data and personal data breaches, including if applicable Customer's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR, by: (a) Implementing and maintaining the Security Measures in accordance with Section 6.1.1 (AIS's Security Measures); (b) Complying with the terms of Section 0 (Data Incidents); and (c) Providing Customer with the Security Documentation in accordance with Section 6.4.1 (Reviews of Security Documentation) and

the information contained in the applicable Agreement including this Data Processing Agreement.

6.2. Data Incidents (Personal Data Breach)

6.2.1. Incident Notification

6.2.1.1. If AIS becomes aware of a Data Incident, AIS will: (a) notify the Customer of the Data Incident promptly and without undue delay; and (b) promptly take reasonable steps to minimize harm and secure Customer Data.

6.2.2. Details of Data Incident

6.2.2.1. Notifications made pursuant to this section will describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and steps AIS recommends Customer take to address the Data Incident.

6.2.3. Delivery of Notification

6.2.3.1. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address or, at AIS's discretion, by direct communication (for example, by phone call or an in-person meeting). The Customer is solely responsible for ensuring that the Notification Email Address is current and valid.

6.2.4. No Assessment of Customer Data by AIS

6.2.4.1. AIS will not assess the contents of Customer Data in order to identify information subject to any specific legal requirements. Customer is solely responsible for complying with incident notification laws applicable to the Customer and fulfilling any third-party notification obligations related to any Data Incident(s).

6.2.5. No Acknowledgment of Fault by AIS

6.2.5.1. AIS's notification of or response to a Data Incident under this Section 0 (Data Incidents) will not be construed as an acknowledgement by AIS of any fault or liability with respect to the Data Incident.

6.3. Customer's Security Responsibilities and Assessment

6.3.1. Customer's Security Responsibilities

6.3.1.1. Customer agrees that, without prejudice to AIS's obligations under Section 6.1 (AIS's Security Measures, Controls and Assistance) and Section 0 (Data Incidents):

6.3.1.1.1. Customer is solely responsible for its use of the Services, including: (a) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Data; (b) securing the account authentication credentials, systems and devices Customer uses to access the Services; and (c) backing up its Customer Data; and

6.3.1.1.2. AIS has no obligation to protect Customer Data in the event that the Customer elects to store or transfer outside of AIS's and its Sub-Processors' systems (for example, offline or on-premise storage).

6.3.2. Customer's Security Assessment.

6.3.2.1. Customer is solely responsible for reviewing the Security Documentation and evaluating for itself whether the Services, the Security Measures and AIS's commitments under this Section 5 (Data Security) will meet Customer's needs, including with respect to any security obligations of Customer under Data Protection Laws and Regulations, as applicable.

6.3.2.2. Customer acknowledges and agrees that the Security Measures implemented and maintained by AIS as set out in Section 6.1.1 (AIS's Security Measures) provide a level of security appropriate to the risk in respect of the Customer Data.

6.4. Reviews and Audits of Compliance

6.4.1. Reviews of Security Documentation

6.4.1.1. Upon Customer's written request, and subject to the confidentiality obligations set forth in the Agreement, AIS shall make available to Customer that is not a competitor of AIS (or

Customer's independent, third-party auditor that is not a competitor of AIS) a copy of AIS's most recent third-party audits or certifications, as applicable.

6.4.2. Customer's Audit Rights

6.4.2.1. If the European Data Protection Legislation applies to the processing of Customer Personal Data, AIS will allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) to verify AIS's compliance with its obligations under this Data Processing Agreement in accordance with Section 6.4.3 (Additional Business Terms for Reviews and Audits). AIS will contribute to such audits as described in this Section 0 (Reviews and Audits of Compliance).

6.4.2.2. Customer may also conduct an audit to verify AIS's compliance with its obligations under this Data Processing Agreement by reviewing the Security Documentation.

6.4.3. Additional Business Terms for Reviews and Audits

6.4.3.1. Customer must send any requests for reviews under Section 6.4.1 or audits under Section 6.4.2(a) or 6.4.2(b) to AIS by postal mail to AIS's office address as indicated on our website's Contact Us section.

6.4.3.2. Following receipt by AIS of a request of audit, AIS and Customer will discuss and agree in advance on: (i) the reasonable date(s) of review under Section 6.4.1; and (ii) the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit under Section 6.4.2(a) or 6.4.2(b).

6.4.3.3. AIS may charge a fee (based on AIS's reasonable costs) for any audit under Section 6.4.2(a) or 6.4.2(b). AIS will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

6.5. AIS may object in writing to an auditor appointed by Customer to conduct any audit under Section 6.4.2(a) or 6.4.2(b) if the auditor is, in AIS's reasonable opinion, not suitably qualified or independent, a competitor of AIS, or otherwise manifestly unsuitable. Any such objection by AIS will require Customer to appoint another auditor or conduct the audit itself.

7. Impact Assessments and Consultations

7.1. Customer agrees that AIS will (taking into account the nature of the processing and the information available to AIS) assist the Customer in ensuring compliance with any obligations of Customer in respect of data protection impact assessments and prior consultation, including if applicable Customer's obligations pursuant to Articles 35 and 36 of the GDPR, by:

7.1.1. providing the Security Documentation in accordance with Section 6.4.1 (Reviews of Security Documentation); and

7.1.2. providing the information contained in the applicable Agreement including this Data Processing Agreement.

8. Data Subject Rights and Data Export

8.1. Access; Rectification; Restricted Processing; Portability

8.1.1. During the applicable Term, AIS will, in a manner consistent with the functionality of the Services, enable the Customer to access, rectify and restrict processing of Customer Data, including via the deletion functionality provided by AIS and to export Customer Data.

8.2. Data Subject Requests

8.2.1. Customer's Responsibility for Requests

8.2.1.1. During the applicable Term, if AIS receives any request from a data subject in relation to the Customer's Personal Data, AIS will advise the data subject to submit his/her request to the Customer, and the Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

8.2.2. AIS's Data Subject Request Assistance

8.2.2.1. The Customer agrees that (taking into account the nature of the processing of Customer Personal Data) AIS will assist the Customer in fulfilling any obligation to respond to requests by data subjects, including if applicable Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, by complying with the commitments set out in Section 7.1 (Access; Rectification; Restricted Processing; Portability) and Section 8.2.1 (Customer's Responsibility for Requests).

9. Data Transfers

9.1. Data Storage and Processing Facilities

9.1.1. Customer agrees that AIS may, subject to Section 9.3 (Transfers of Data Out of the EEA), store and process Customer Data in Malta, Europe and any other country in which AIS or any of its Sub-Processors maintains facilities.

9.1.2. AIS's AIS agrees and warrants:

9.1.2.1. to process the personal data only on behalf of the Customer and in compliance with its instructions and the DPA;

9.1.2.2. that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the Customer and its obligations under the contract;

9.1.2.3. that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

9.1.2.4. that it will promptly notify the Customer about: (a) any accidental or unauthorised access; and (b) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

9.1.2.5. to deal promptly and properly with all inquiries from the Customer relating to its processing of the personal data subject to the transfer;

9.1.2.6. to make available to the data subject upon request a copy of the DPA, or any existing contract for sub-processing, unless the contracts contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the Customer;

9.1.2.7. that, in the event of sub-processing, it has previously informed the Customer and obtained its prior written consent;

9.1.2.8. that the processing services by the sub-processor will be carried out in accordance with Section 10.

9.2. Customer's Transfer Obligations

9.2.1. The Customer agrees and warrants:

9.2.1.1. that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the Customer is established) and does not violate the relevant provisions of that State;

9.2.1.2. that it has instructed and throughout the duration of the personal data-processing services will instruct the data processor to process the personal data transferred only on the Customer's behalf and in accordance with the applicable data protection law and the DPA;

9.2.1.3. that the data processor will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

9.2.1.4. that it will ensure compliance with the security measures;

9.2.1.5. that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

9.2.1.6. to make available to the data subjects upon request a copy of the DPA, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the DPA, unless the DPA or the contract contain commercial information, in which case it may remove such commercial information;

9.2.1.7. that, in the event of sub-processing, the processing activity is carried out in accordance with Section 10 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as AIS under the DPA.

9.3. Transfers of Data Out of the EEA

9.3.1. AIS shall store the Customer's Personal Data within the European Economic Area (EEA), or outside of the EEA in accordance with the Privacy Shield Framework and Principles and/or the Standard Contractual Clauses. AIS will obtain prior written consent from the Customer should it store Personal Data outside of the EEA.

9.3.2. In the event of such consent, AIS will ensure that this Personal Data will be stored and processed in full compliance with Data Protection Laws. Furthermore, AIS will ascertain that the Technical and Organisational Measures are in place and apply to AIS and its Authorised Sub-contractors. By agreeing to this DPA, the Customer declares that they consent to the storage of Personal Data as defined in Section 14.

9.4. Data Storage Information

9.4.1. AIS's data storage is hosted on European servers provided by Microsoft. Further information can be found here: https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located

10. Sub-Processors

10.1. Consent to Sub-Processor Engagement

10.1.1. Customer specifically authorises the engagement of AIS's Affiliates as Sub-Processors. In addition, AIS and AIS's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services ("Third Party Sub-Processors"). A list of AIS's current Authorised Sub-Processors is found in Appendix 1.

10.2. Requirements for Sub-Processor Engagement

10.2.1. When engaging any Sub-Processor, AIS will ensure via a written contract that:

10.2.1.1. the Sub-Processor only accesses and uses Customer Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the applicable Agreement (including this Data Processing Agreement); and

10.2.1.2. if the GDPR applies to the processing of Customer Personal Data, the data protection obligations set out in Article 28(3) of the GDPR, as described in this Data Processing Agreement, are imposed on the Sub-Processor; and

10.2.1.3. remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Sub-Processor.

10.3. Opportunity to Object to Sub-Processor Changes

10.3.1. When any new Third Party Sub-Processor is engaged during the applicable Term, AIS will, at least 30 days before the new Third Party Sub-Processor processes any Customer Data, inform the Customer of the engagement (including the name and location of the relevant Sub-Processor and the activities it will perform) by sending an email to the Notification Email Address.

10.3.2. Customer may object to any new Third Party Sub-Processor by terminating the applicable Agreement immediately upon written notice to AIS, on condition that the Customer provides such notice within 90 days of being informed of the engagement of the Sub-Processor. This termination right is the Customer's sole and exclusive remedy if the Customer objects to any new Third Party Sub-Processor.

11. Obligation after the Termination of Service

11.1. The Parties agree that on the termination of the provision of the Services, AIS and the sub-processor shall, at the choice of the Customer, return all the personal data transferred and the copies thereof to the Customer or shall destroy all the personal data and certify to the Customer that it has done so, unless legislation imposed upon AIS prevents it from returning or destroying all or part of the personal data transferred. In that case, AIS warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12. Effect of Addition

12.1. To the extent of any conflict or inconsistency between the terms of this Data Processing Agreement and the remainder of the applicable Agreement, the terms of this Data Processing Agreement will govern. Subject to the amendments in this Data Processing Agreement, such Agreement remains in full force and effect.

13. Governing Law

13.1. This Agreement and DPA shall be governed by and construed in accordance with the laws of Malta and shall be subject to the exclusive jurisdiction of the Courts of Malta.

SIGNED on behalf of **THE CUSTOMER**	Signature: Name: Date:
SIGNED on behalf of **AIS Technology Ltd** **THE PROCESSOR**	Signature: Name: Date:

Appendix 1

14. List of Approved Sub-Processors

Sub-Processor	Nature of Services	Relevant Data Processed	Location
Microsoft	Hosting, Network and Database services on Microsoft Azure	All information processed by AIS's subscription-based services is hosted on Microsoft Azure	Netherlands, Ireland, Europe
Google Analytics	Usage analytics	Information regarding page visits, location information, visitor data, device type	United States of America
SendGrid	Automated email service for notifications	Customer notification email address, subject, email status	United States of America
Mailchimp	Email marketing mailing lists & distribution	Name, surname, email address	United States of America

15. Categories of Data Processed

15.1. Personal Data processed may include, but is not limited to name, surname, user ID, employee ID, contact information (email address, phone, and physical business address), employment details (company, job title, department) and other data added into the account in Customer's sole discretion.

15.2. Special categories of data (if appropriate)

15.2.1. Special data processed may include biometric data processed for the sole purpose of providing the Services as stipulated in this DPA. The Customer bears the responsibility to obtain explicit consent of the data subject for the purposes of processing of the Special data. AIS process Special data solely for the purpose of providing the Services as stipulated in this DPA on the basis that such services are necessary for the purposes of the legitimate interests pursued by the Customer, specifically for the purposes of preventing fraud, as supported by recital 52 of GDPR. Appendix 3 details the specific nature by which Special data is processed.

Appendix 2

16. Technical and Organisational Measures

16.1. This Appendix forms part of the DPA. This Appendix provides an overview of the measures implemented by AIS to ensure a security level appropriate to the risks related to the processing of the Personal Data required for the provision of the Services. The Technical and Organisational measures vary based on the nature of the Services provided, according to whether the Service is a Software-as-a-Service offering, On-Premise offering and other services related to such offerings.

16.2. General Controls

16.2.1. The following technical and organisational measures have been implemented by AIS to ensure the security and availability of the systems and operations required to provide services to our Customers. These measures are defined below:

16.2.1.1. Role-based security groups and access on all servers, virtual machines and devices

16.2.1.2. Electronic security systems, including Access Control, CCTV and Intruder Alarm systems at AIS offices

16.2.1.3. Encrypted data backup for disaster recovery

16.2.1.4. IT security systems including firewall, anti-malware, virus scanners, mail and web content filters

16.3. Personnel

16.3.1. AIS shall take reasonable steps to ensure that no person shall be appointed by AIS to process Personal Data unless that person:

16.3.1.1. is competent and qualified to perform the specific tasks assigned to him by AIS;

16.3.1.2. has been authorised by AIS; and

16.3.1.3. has been instructed by AIS in the requirements relevant to the performance of the obligations of AIS under this DPA, in particular the limited purpose of the data processing.

16.4. Copy Control

16.4.1. AIS shall not make copies of Personal Data, provided, however, that AIS may retain copies of Personal Data provided to it for backup and archive purposes.

16.5. Security Controls – Software-as-a-Service solutions

16.5.1. The Software-as-a-Service includes a variety of security controls that provide the Customer with industry-standard security of the Service for its own use. These controls include:

16.5.1.1. Unique User identifiers (User IDs) to ensure that activities can be attributed to the responsible individual.

16.5.1.2. Controls to require browser re-opening after several consecutive failed login attempts.

16.5.1.3. Controls to ensure generated initial passwords must be reset on first use.

16.5.1.4. Controls to terminate a User session after a period of inactivity.

16.5.1.5. Password length controls.

16.5.1.6. Password complexity requirements (requires letters and numbers).

16.6. Security Procedures, Policies and Logging - Software-as-a-Service solutions

16.6.1. The Services are operated in accordance with the following procedures to enhance security:

16.6.1.1. User passwords are stored using a one-way hashing algorithm (SHA-512) and are never transmitted unencrypted.

16.6.1.2. Some of user access log entries will be maintained, containing date, time, User ID, URL executed or entity ID operated on, operation performed (viewed, edited, etc.)

16.6.1.3. If there is suspicion of inappropriate access, AIS or its Sub-processor can provide Customer log entry records to assist in forensic analysis. This service will be provided to Customer on a time and materials basis.

16.6.1.4. Passwords are not logged under any circumstances.

16.6.1.5. Certain administrative changes to the Services are tracked in an area known as “Audit Trail” and are available for viewing by Customer’s system administrator.

16.6.1.6. User can request to reset password to the Customer’s system administrator.

16.7. User Authentication - Software-as-a-Service solutions

16.7.1. Access to the Services requires a valid User ID and password combination, which are encrypted via SSL while in transmission. Following a successful authentication, a random session ID is generated and stored in the user’s browser to preserve and track session state.

16.8. Incident Management - Software-as-a-Service solutions

16.8.1. AIS maintains security incident management policies and procedures. AIS will promptly notify Customer in the event AIS becomes aware of an actual or reasonably suspected unauthorised disclosure of Personal Data.

16.9. Reliability and Backup - Software-as-a-Service solutions

16.9.1. All networking components, Web servers and application servers that are part of the Software-as-a-Service platform are configured and replicated with Microsoft Azure services to keep your data safe for possible backup purposes.

16.10. Disaster Recovery - Software-as-a-Service solutions

16.10.1. AIS will ensure that its Sub-processor that stores Customer Data has disaster recovery plans in place and tests them at least once per year.

16.11. Data Encryption - Software-as-a-Service solutions

16.11.1. The Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Services, including 256-bit SSL Certificates and 2048-bit RSA public keys at a minimum.

16.12. System Changes and Enhancements - Software-as-a-Service solutions

16.12.1. AIS plans to enhance and maintain the Services during the term of the Agreement. Security controls, procedures, policies and features may change or be added. AIS will provide security controls that deliver a level of security protection that is not materially lower than that provided as of the Effective Date.

16.13. Security Controls – On-premise solutions

16.13.1. AIS’s On-Premise software is located at the Customer’s network and IT infrastructure, or at a 3rd party hosting environment sub-contracted by the Customer. As a result, Technical and Organisational measures to protect Personal data are the responsibility of the Customer and/or its sub-contractor.

Appendix 3

17. Time & Attendance Devices including Biometric Devices

17.1. For the purposes of delivering Time & Attendance solutions to various businesses, AIS offer biometric terminals to record employee attendance. Various forms of identification technologies exist which include hand recognition, face recognition, fingerprint recognition, PIN code and RFID card technology.

17.2. As defined in Section 2, Personal Data includes any information that can be used to distinguish, identify or contact you. This section will demonstrate that whilst biometric identification is used to identify a user to the device, the biometric information is transferred into data in the form of an algorithm and cannot be re-engineered to distinguish, identify or contact any individual.

17.3. Hand Recognition

17.3.1. Hand recognition devices use hand geometry technology, i.e. the size and shape of a user's hand to confirm identity. Over 90 distinct measurements are made each time to verify a user. These include length, width, thickness and surface area. It does not read fingerprints or palm prints. AIS Technology deliver hand recognition devices provided by Allegion.

17.3.2. User enrolment works as follows:

- User presents hand into the device
- The image of the hand is captured by the device
- The hand geometric image is converted into a data key through an algorithm proprietary to the supplier (Allegion)
- The resulting template is stored on the device

17.3.3. User verification works as follows:

- User enters ID or credential
- User presents hand into the device
- The image of the hand is captured by the device
- The hand geometric image is converted into a data key through an algorithm proprietary to the supplier (Allegion).
- An instant comparison is made between the two templates to confirm if a match is present.
- The result (Identity verified or rejected) is sent to the T&A software application.

17.3.4. At no point in time is the original biometric data captured, managed or stored by AIS. Furthermore, the algorithm by which the biometric image is converted into data is managed by the supplier and inaccessible to AIS and/or third parties. Therefore, no biometric information of any user is captured, stored and managed within the entire Time & Attendance solution. The biometric image cannot be reverse engineered to produce the individual's hand pattern.

17.4. Face Recognition

17.4.1. Face recognition terminals capture an image of an individuals' facial characteristics. AIS Technology deliver face recognition devices provided by FingerTec.

17.4.2. User enrolment works as follows:

- User presents face in front of the device
- The image of the face is captured by the device
- The facial image is converted into a data key through an algorithm proprietary to the supplier (FingerTec).
- The resulting template is stored on the device

17.4.3. User verification works as follows:

- User enters ID or credential
- User presents face in front of the device
- The image of the face is captured by the device
- The facial image is converted into a data key through an algorithm proprietary to the supplier (FingerTec).

- An instant comparison is made between the two templates to confirm if a match is present.
- The result (Identity verified or rejected) is sent to the T&A software application.

17.4.4. At no point in time is the original biometric data captured, managed or stored by AIS. Furthermore, the algorithm by which the biometric image is converted into data is encrypted and managed by the supplier and inaccessible to AIS and/or third parties. Therefore, no biometric information of any user is captured, stored and managed within the entire Time & Attendance solution. The biometric image cannot be reverse engineered to produce the individual's facial pattern.

17.5. Fingerprint Recognition

17.5.1. Fingerprint recognition terminals uses an individuals' fingerprint characteristics to identify a user. Minutia points measuring the location of a fingerprint's ridges and valleys are extracted and converted into data. AIS Technology deliver fingerprint recognition devices provided by FingerTec.

17.5.2. User enrolment works as follows:

- User presents finger in the device
- The image of the fingerprint is captured by the device
- The minutia points are extracted from the image, and converted into a data key through an algorithm proprietary to the supplier (FingerTec)
- The resulting template is stored on the device.

17.5.3. User verification works as follows:

- User enters ID or credential
- User presents fingerprint in the device
- The image of the fingerprint is captured by the device
- The minutia points are extracted from the fingerprint image and converted into a data key through an algorithm proprietary to the supplier (FingerTec).
- An instant comparison is made between the two templates to confirm if a match is present.
- The result (Identity verified or rejected) is sent to the T&A software application.

17.5.4. At no point in time is the original biometric data captured, managed or stored by AIS. Furthermore, the algorithm by which the biometric image is converted into data is managed by the supplier and inaccessible to AIS and/or third parties. Therefore, no biometric information of any user is captured, stored and managed within the entire Time & Attendance solution. The biometric image cannot be reverse engineered to produce the individual's fingerprint pattern.

17.6. Fingerprint-On-Card Technology

17.6.1. Fingerprint-on-card technology is available on a select range of terminals provided by Fingertec. The technology works by storing a user's fingerprint template inside the storage capacity of a MIFARE card. This technology ensures that the biometric template is kept by the user at all times.

17.6.2. User enrolment works as follows:

- User presents finger in the device
- The image of the fingerprint is captured by the device
- The minutia points are extracted from the image, and converted into a data key through an algorithm proprietary to the supplier (FingerTec).
- The user card is presented to the device
- The resulting template is stored on the card only.

17.6.3. User verification works as follows:

- User enters ID or credential
- User presents card to the device
- User presents fingerprint in the device
- The image of the fingerprint is captured by the device

- The minutia points are extracted from the fingerprint image and converted into a data key through an algorithm proprietary to the supplier
- An instant comparison is made between the two templates to confirm if a match is present.
- The result (Identity verified or rejected) is sent to the T&A software application.
- No biometric template is stored on the device