Data Processing Addendum to Koolsite's Service Contract

This Data Processing Amendment to provide Cloud Service Product Contract including its appendices will be effective and replace any previously applicable data processing amendment or, in the case of a Complementary Product Contract, any terms previously applicable to privacy, data processing and/or data security.

1. **Introduction**.

- This Data Processing Amendment reflects the parties' Contract with respect to the terms governing the processing and security of Client Data under the applicable Contract.

2. **Definitions**.

- 2.1. Capitalized terms used but not defined in this Data Processing Amendment have the meanings given in the General Data Protection Regulation 2016/679 (GDPR)
  - "**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 much 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.
  - "**Amendment Effective Date**" means, as applicable:
    - (a) 25 May 2018, if the Client had a valid Contract at this date and agrees to continue to make use of the established services; or
    - (b) the date on which the Client signs a Service Contract and agrees to this Data Processing Amendment, if such date is after 25 May 2018.
    - "**Complementary Service Contract**" means: any other Contract under which Koolsite agrees to provide services to Client; or any other Contract that incorporates this Data Processing Amendment by reference or states that it will apply if accepted by Client.
    - "**Client Data**" means data submitted, stored, sent or received via the Services by Client, its Affiliates or End Users.
    - "**Client Personal Data**" means personal data contained within the Client Data.
    - "**Data Incident**" means a breach of Koolsite's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Client Data on systems managed by or otherwise controlled by Koolsite. "Data Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Client Data, including unsuccessful log-in attempts, pings,

port scans, denial of service attacks, and other network attacks on firewalls or networked systems.
    - "**European Data Protection Legislation**" means GDPR.
    - "**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.
    - "**Notification Email Address**" means the email address(es) designated by Client to receive certain notifications from Koolsite.
    - "**Security Documentation**" means all documents and information made available by Koolsite related to data security provided by subprocessor.
    - "**Security Measures**" has the meaning given in Section 7.1.1 (Koolsite's Security Measures).
    - "**Services**" means the services contracted by the client in Cloud Mode as described in the corresponding Service Contract.
    - "**Subprocessors**" means third parties authorized under this Data Processing Amendment to have logical access to and process Client Data to provide parts of the Services and related technical support.
    - "**Term**" means the period from the Amendment Effective Date until the end of Koolsite's provision of the Services under the applicable Contract, including, if applicable, any period during which provision of the Services may be suspended and any post-termination period during which Koolsite may continue providing the Services for transitional purposes.
  - 2.2. The terms "personal data", "data subject", "processing", "controller", "processor" and "supervisory authority" as used in this Data Processing Amendment have the meanings given in the GDPR.

3. **Duration of Data Processing Amendment**. This Data Processing Amendment will take effect on the Amendment Effective Date and, notwithstanding expiry of the Term, remain in effect until, and automatically expire upon, deletion of all Client Data by Koolsite as described in this Data Processing Amendment.

4. **Scope of Data Protection Legislation**.

- The Scope of Data Protection Legislation is as defined in the GDPR.

5. **Processing of Data**.

- 5.1 **Roles and Regulatory Compliance; Authorization**.

    - 5.1.1. Processor and Controller Responsibilities. If the European Data Protection Legislation applies to the processing of Client Personal Data, the parties acknowledge and agree that:
        - (a) the subject matter and details of the processing are described in Appendix 1;
        - (b) Koolsite is a processor of that Client Personal Data under the European Data Protection Legislation;
        - (c) Client is a controller or processor, as applicable, of that Client Personal Data under the European Data Protection Legislation; and
        - (d) each party will comply with the obligations applicable to it under the European Data Protection Legislation with respect to the processing of that Client Personal Data.
    - 5.1.2. Authorization by Third Party Controller. If the European Data Protection Legislation applies to the processing of Client Personal Data and Client is a processor, Client warrants to Koolsite that Client's instructions and actions with respect to that Client Personal Data, including its appointment of Koolsite as another processor, have been authorized by the relevant controller.
- 5.2 **Scope of Processing**.
    - 5.2.1 Client's Instructions. By entering into this Data Processing Amendment, Client instructs Koolsite to process Client Personal Data only in accordance with applicable law: (a) to provide the Services and related technical support; (b) as further specified via Client's use of the Services (c) as documented in the form of the applicable Contract, including this Data Processing Amendment; and (d) as further documented in any other written instructions given by Client and acknowledged by Koolsite as constituting instructions for purposes of this Data Processing Amendment.
    - 5.2.2 Koolsite's Compliance with Instructions. As from the Full Activation Date, Koolsite will comply with the instructions described in Section 5.2.1 (Client's Instructions) (including regarding data transfers) unless EU or EU Member State law to which Koolsite is subject requires other processing of Client Personal Data by Koolsite, in which case Koolsite will inform Client (unless that law prohibits Koolsite from doing so on important grounds of public interest) via the Notification Email Address.

6. **Data Deletion**.

- 6.1. **Deletion During Term**. Koolsite will enable Client and/or End Users to delete Client Data during the applicable Term in a manner consistent with the functionality of the Services. If Client or an End User uses the Services to delete any Client Data during the applicable Term and the Client Data cannot be recovered by Client or an End User, this use will constitute an instruction to Koolsite to delete the relevant Client Data from Koolsite's systems in accordance with applicable law. Koolsite will comply with this instruction as soon as reasonably practicable and within a maximum period of 90 days, unless EU or EU Member State law requires storage.

- 6.2. **Deletion on Term Expiry**. On expiration of the applicable Term, Client instructs Koolsite to delete all Client Data (including existing copies) from Koolsite's systems in accordance with applicable law. Koolsite will comply with this instruction as soon as reasonably practicable and within a maximum period of 90 days, unless EU or EU Member State law requires storage. Without prejudice to Section 9.1 (Access; Rectification; Restricted Processing; Portability), Client acknowledges and agrees that Client will be responsible for exporting, before the applicable Term expires, any Client Data it wishes to retain afterwards.

7. **Data Security**.

- 7.1. **Koolsite's Security Measures, Controls and Assistance**.
  - 7.1.1. Koolsite's Security Measures. Koolsite will implement and maintain technical and organizational measures to protect Client Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 2 (the "Security Measures"). These include measures to encrypt personal data; to help ensure ongoing confidentiality, integrity, availability and resilience of Koolsite's systems and services; to help restore timely access to personal data following an incident; and for regular testing of effectiveness. Koolsite 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.
  - 7.1.2. Security Compliance by Koolsite Staff. Koolsite will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance, including ensuring that all persons authorized to process Client Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
  - 7.1.3. Additional Security Controls. In addition to the Security Measures, Koolsite will make the Additional Security Controls available to: (a) allow Client to take steps to secure Client Data; and (b) provide Client with information about securing, accessing and using Client Data.
  - 7.1.4. Koolsite's Security Assistance. Client agrees that Koolsite will (considering the nature of the processing of Client Personal Data and the information available to Koolsite) assist Client in ensuring compliance with any of Client's obligations in respect of security of personal data and personal data breaches, including if applicable Client's obligations pursuant to Articles 32, 33 and 34 of the GDPR, by:
    - (a) implementing and maintaining the Security Measures in accordance with Section 7.1.1 (Koolsite's Security Measures);

        - (b) making the Additional Security Controls available to Client in accordance with Section 7.1.3 (Additional Security Controls);
        - (c) complying with the terms of Section 7.2 (Data Incidents);
- 7.2. **Data Incidents**.
    - 7.2.1. Incident Notification. If Koolsite becomes aware of a Data Incident, Koolsite will: (a) notify Client of the Data Incident promptly and without undue delay; and (b) promptly take reasonable steps to minimize harm and secure Client Data.
    - 7.2.2. Details of Data Incident. 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 Koolsite recommends Client take to address the Data Incident.
    - 7.2.3. Delivery of Notification. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address or, at Koolsite's discretion, by direct communication (for example, by phone call or an in-person meeting). Client is solely responsible for ensuring that the Notification Email Address is current and valid.
    - 7.2.4. No Assessment of Client Data by Koolsite. Koolsite will not assess the contents of Client Data to identify information subject to any specific legal requirements. Client is solely responsible for complying with incident notification laws applicable to Client and fulfilling any third party notification obligations related to any Data Incident(s).
    - 7.2.5. No Acknowledgment of Fault by Koolsite. Koolsite's notification of or response to a Data Incident under this Section 7.2 (Data Incidents) will not be construed as an acknowledgement by Koolsite of any fault or liability with respect to the Data Incident.
- 7.3. **Client's Security Responsibilities and Assessment**.
    - 7.3.1. Client's Security Responsibilities. Client agrees that, without prejudice to Koolsite's obligations under Section 7.1 (Koolsite's Security Measures, Controls and Assistance) and Section 7.2 (Data Incidents):
        - (a) Client is solely responsible for its use of the Services, including:
            - (i) making appropriate use of the Services and the Additional Security Controls to ensure a level of security appropriate to the risk in respect of the Client Data;
            - (ii) securing the account authentication credentials, systems and devices Client uses to access the Services; and
            - (iii) backing up its Client Data; and
        - (b) Koolsite has no obligation to protect Client Data that Client elects to store or transfer outside of Koolsite's and its Subprocessors' systems (for example, offline or on-premise storage), or to protect Client Data by implementing or

        maintaining Additional Security Controls except to the extent Client has opted to use them.

    - 7.3.2. Client’s Security Assessment.
        - (a) Client is solely responsible for reviewing the Security Documentation and evaluating for itself whether the Services, the Security Measures, the Additional Security Controls and Koolsite’s commitments under this Section 7 (Data Security) will meet Client’s needs, including with respect to any security obligations of Client under the European Data Protection Legislation
        - (b) Client acknowledges and agrees that (considering the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Client Personal Data as well as the risks to individuals) the Security Measures implemented and maintained by Koolsite as set out in Section 7.1.1 (Koolsite’s Security Measures) provide a level of security appropriate to the risk in respect of the Client Data.

8. **Impact Assessments and Consultations**. Client agrees that Koolsite will (considering the nature of the processing and the information available to Koolsite) assist Client in ensuring compliance with any obligations of Client in respect of data protection impact assessments and prior consultation, including if applicable Client’s obligations pursuant to Articles 35 and 36 of the GDPR, by:

- (a) providing the Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls); and
- (b) providing the information contained in the applicable Contract including this Data Processing Amendment.

9. **Data Subject Rights; Data Export**.

- 9.1. **Access; Rectification; Restricted Processing; Portability**. During the applicable Term, Koolsite will, in a manner consistent with the functionality of the Services, enable Client to access, rectify and restrict processing of Client Data, including via the deletion functionality provided by Koolsite as described in Section 6.1 (Deletion During Term), and to export Client Data.
- 9.2. **Data Subject Requests**.
    - 9.2.1. Client’s Responsibility for Requests. During the applicable Term, if Koolsite receives any request from a data subject in relation to Client Personal Data, Koolsite will advise the data subject to submit his/her request to Client, and Client will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.
    - 9.2.2. Koolsite’s Data Subject Request Assistance. Client agrees that (taking into account the nature of the processing of Client Personal Data) Koolsite will assist Client in fulfilling any obligation to respond to requests by data subjects, including if applicable Client’s

obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, by:

  - (a) providing the Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls); and
  - (b) complying with the commitments set out in Section 9.1 (Access; Rectification; Restricted Processing; Portability) and Section 9.2.1 (Client's Responsibility for Requests).

10. **Data Transfers**.

Data Storage and Processing Facilities. Client agrees that Koolsite may transfer personal data to a third country or an international organisation if the European Commission had decided that the third country, a territory, or one or more specific sectors of that third country, or the international organisation in consideration, guarantees an adequate level of protection. This transference does not require specific authorisation.

11. **Subprocessors**.

- 11.1. **Consent to Subprocessor Engagement**. Client specifically authorizes the engagement of Koolsite's Affiliates as Subprocessors.
- 11.2. **Information about Subprocessors**. Information about Subprocessors, including their functions and locations can be requested by email to: support@koolsite.co.uk
- 11.3. **Requirements for Subprocessor Engagement**. When engaging any Subprocessor, Koolsite will:
  - (a) ensure via a written contract that:
    - (i) the Subprocessor only accesses and uses Client Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the applicable Contract (including this Data Processing Amendment); and
    - (ii) if the GDPR applies to the processing of Client Personal Data, the data protection obligations set out in Article 28(3) of the GDPR, as described in this Data Processing Amendment, are imposed on the Subprocessor; and
    - (b) remains fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.
- 11.4. **Opportunity to Object to Subprocessor Changes**.
    - (a) When any new Third Party Subprocessor is engaged during the applicable Term, Koolsite will, at least 30 days before the new Third Party Subprocessor processes any Client Data, inform Client of the engagement (including the name and location of the relevant subprocessor and the activities it will perform) by sending an email to the Notification Email Address.
    - (b) Client may object to any new Third Party Subprocessor by terminating the applicable Contract immediately upon written notice to Koolsite, on condition that Client provides such notice within 90 days of being informed of the

engagement of the subprocessor as described in Section 11.4(a). This termination right is Client's sole and exclusive remedy if Client objects to any new Third Party Subprocessor.

12. **Koolsite's Processing Records**. Client acknowledges that Koolsite is required under the GDPR to:

- (a) collect and maintain records of certain information, including the name and contact details of each processor and/or controller on behalf of which Koolsite is acting and, where applicable, of such processor's or controller's local representative and data protection officer; and
- (b) make such information available to the supervisory authorities. Accordingly, if the GDPR applies to the processing of Client Personal Data, Client will, where requested, provide such information to Koolsite and ensure that all information provided is kept accurate and up-to-date.

13. **Effect of Amendment**. To the extent of any conflict or inconsistency between the terms of this Data Processing Amendment and the remainder of the applicable Contract, the terms of this Data Processing Amendment will govern. Subject to the amendments in this Data Processing Amendment, such Contract remains in full force and effect. For clarity, if Client has entered more than one Contract, this Data Processing Amendment will amend each of the Contracts separately.

Appendix 1: Subject Matter and Details of the Data Processing

Subject Matter

Provision of the Services by Koolsite and related technical support to Client.

Duration of the Processing

The applicable Term plus the period from expiry of such Term until deletion of all Client Data by Koolsite in accordance with the Data Processing Amendment.

Nature and Purpose of the Processing

Koolsite will process Client Personal Data submitted, stored, sent or received by Client, its Affiliates or End Users via the Services for the purposes of providing the Services and related technical support to Client in accordance with the Data Processing Amendment.

Categories of Data

Personal data submitted, stored, sent or received by Client, its Affiliates or End Users via the Services may include the following categories of data: user IDs, email, documents, images, calendar entries, tasks and other data.

Data Subjects

Personal data submitted, stored, sent or received via the Services may concern the following categories of data subjects: End Users including Client’s employees and contractors; the personnel of Client’s Clients, suppliers and subcontractors; and any other person who transmits data via the Services, including individuals collaborating and communicating with End Users.

Appendix 2: Security Measures

As from the Amendment Effective Date, Koolsite will implement and maintain the Security Measures set out in this Appendix 2 to the Data Processing Amendment. Koolsite may update or modify such 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.

IT Infrastructure

IaaS

Koolsite offers the Services using an Informatics Infrastructure in mode IaaS (Infrastructure as a Service), provided by a top-level service provider that includes:

Servers
Storage
Communications

The Cloud Services provider is IBM and the Data Centers used are in London, UK and Milan, Italy.

The security measures and data protection support provided by the Cloud Infrastructure Provider in conformity with GDPR, can be consulted in the following link:

https://www-05.ibm.com/support/operations/zz/en/dpa.html

PaaS and SaaS

Koolsite provides its services in mode SaaS (Software as a Service) and manages the Software components at the PaaS level (Platform as a Service): Database Engine, Operating System, Applications Servers, Backup and Restore, Communications.

The following aspects are implemented at the PaaS level:

Database: Encryption supported at the level of the Database Manager using the AES standard (Advanced Encryption Standard) of all the Application database tables.

Communication between Application Servers and Database: Secure connection between the JDBC driver and the Database Server using SSL (Secure Socket Layer).

SSL Digital Certificates for the Web Server.

At the Application SaaS level:

The communications between the end users and Koolsite's servers are made through a TLS (Transport Layer Security) technology connection.

Personnel Security.

Koolsite personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Koolsite conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable labour law and statutory regulations.

Personnel are required to execute a confidentiality Contract and must acknowledge receipt of, and compliance with, Koolsite's confidentiality and privacy policies. Personnel are provided with health and safety training. Personnel handling Client Data are required to complete additional requirements appropriate to their role. Koolsite's personnel will not process Client Data without authorization.

Subprocessor Security.

Before admitting Subprocessors, Koolsite conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Koolsite has assessed the risks presented by the Subprocessor, then subject always to the requirements set out in Section 11.3 (Requirements for Subprocessor Engagement) of this Data Processing Amendment, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.