DATA PROTECTION ADDENDUM

This Data Protection Addendum ("**DPA**") is supplemental to the Agreement between you ("**Supplier**") and Iron Mountain (UK) Plc ("**Customer**") for the Supply of Goods and/or Services ("**Agreement**") between the Customer and the Supplier.

If any terms and conditions contained herein are in conflict with the terms and conditions set forth in the Agreement, the terms and conditions set forth in this Addendum shall be deemed to be the controlling terms and conditions to the extent of such conflict only. Unless specifically defined herein, all capitalised terms shall have the same meanings as are given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

The parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Agreement.

1. **Definitions**

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "**Authorised Subprocessors**" means any Subprocessors consented to in writing by the Customer in accordance with section 6.1;

1.1.2 "**Customer Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Customer, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.3 "**Customer Personal Data**" means the data described in Annex 1 and any other Personal Data Processed by Supplier or any Subprocessor on behalf of the Customer or any Customer Affiliate pursuant to or in connection with the Agreement.;

1.1.4 "**Data Protection Laws**" means in relation to any Personal Data which is Processed in the performance of the Agreement, the EU Data Protection Directive 95/46/EC as amended from time to time as will be replaced and superseded on 25 May 2018 by the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), in each case together with all laws implementing or supplementing the same and any other applicable data protection or privacy laws;

1.1.5 "**EEA**" means the European Economic Area;

1.1.6 "**Process/Processing**", "**Data Controller**", "**Data Processor**", "**Data Subject**", **"Personal Data", "Personal Data Breach"** and "**Special Categories of Personal Data**" shall have the same meaning as in the Data Protection Laws;

1.1.7 "**Restricted Country"** means a country which (i) is not a Member State of the European Union; and (ii) is not approved by the European Commission as ensuring an adequate level of protection, in accordance with the Data Protection Laws.

1.1.8 "**Services**" means any goods and/or services provided to the Customer pursuant to ther Agreement;

1.1.9 "**Standard Contractual Clauses**" means the standard contractual clauses for the transfer of personal data to Processors established in third countries, as approved by the European Commission in Decision 2010/87/EU, or any set of

clauses approved by the European Commission which amends, replaces or supersedes these;

1.1.10 "**Subprocessor**" means any Data Processor (including any third party and any Supplier Affiliate) appointed by Supplier to Process Customer Personal Data on behalf of the Customer or any Customer Affiliate;

1.1.11 "**Supervisory Authority**" means (a) an independent public authority which is established by a Member State pursuant to Article 51 GDPR; and (b) any similar regulatory authority responsible for the enforcement of Data Protection Laws; and

1.1.12 "**Supplier Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Supplier, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

2. Data Processing Terms

2.1 In the course of providing the Services to the Customer pursuant to the Agreement, Supplier may Process Customer Personal Data on behalf of the Customer or any Customer Affiliate as per the terms of this Addendum. Supplier agrees to comply with the following provisions with respect to any Customer Personal Data submitted by or for the Customer or any Customer Affiliate in connection with the Services or otherwise collected and Processed by or for the Customer or any Customer Affiliate by Supplier or any Supplier Affiliate.

3. Processing of the Customer Personal Data

3.1 Supplier shall only Process the types of Customer Personal Data relating to the categories of Data Subjects for the purposes of the Agreement (and for the specific purposes) in each case as set out in Annex 1 to this Addendum and shall not Process, transfer, modify, amend or alter the Customer Personal Data or disclose or permit the disclosure of the Customer Personal Data to any third party other than in accordance with the Customer's prior written approval (whether in the Agreement or otherwise) unless Processing is required by EU or Member State law to which Supplier is subject, in which case Supplier shall to the extent permitted by such law inform the Customer in writing of that legal requirement before Processing that Personal Data.

4. Supplier Personnel

4.1 Supplier shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to access the relevant Customer Personal Data, as strictly necessary for the purposes set out in section 3.1 above in the context of that individual's duties to Supplier, ensuring that all such individuals:

4.1.1 are informed of the confidential nature of the Customer Personal Data and are aware of Supplier's obligations under this Addendum and the Agreement in relation to the Customer Personal Data;

4.1.2 have undertaken appropriate training in relation to the Data Protection Laws;

4.1.3 are subject to confidentiality undertakings or professional or statutory obligations of confidentiality; and

4.1.4 are subject to user authentication and log-on processes when accessing the Customer Personal Data.

5. **Security**

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Supplier shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

5.1.1 the pseudonyimisation and encryption of the Customer Personal Data;

5.1.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

5.1.3 the ability to restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident; and

5.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

5.2 Without limitation to section 5.1, Supplier shall implement and maintain each of the technical and organisational measures listed in Annex 2 (Technical and Organisational Measures).

5.3 In assessing the appropriate level of security, Supplier shall take account in particular of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

5.4 Customer may also provide written notice to Supplier if in the reasonable opinion of Customer the technical and organisational measures set out in Annex 2 need to be changed to take account of a change of Data Protection Law and Supplier shall promptly implement such changes at no additional cost to Customer. Such written notice shall include a description of the change of law and details of the required change to Annex 2.

5.5 Supplier shall, at its own expense, make changes to the technical and organisational measures set out in Annex 2, as necessary to ensure ongoing compliance with clause 5.1, including without limitation following receipt of a written notice from Customer pursuant to clause 5.4 above, by providing at least 10 days written notice to Customer.

6. **Subprocessing**

6.1 Supplier shall not engage any Data Processors to Process Customer Personal Data other than with the prior written consent of the Customer, which the Customer may refuse in its absolute discretion.

6.2 With respect to each Subprocessor, Supplier shall:

6.2.1 provide the Customer with full details of the Processing to be undertaken by the each Subprocessor;

6.2.2 carry out adequate due diligence on each Subprocessor to ensure that it is capable of providing the level of protection for the Customer Personal Data as is required by this Addendum including without limitation sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of GDPR and this Addendum;

6.2.3 include terms in the contract between Supplier and each Subprocessor which are equivalent to those set out in this Addendum. Upon request, Supplier shall

provide a copy of its agreements with Subprocessors to the Customer for its review;

6.2.4 insofar as that contract involves the transfer of Customer Personal Data (as consented to by the Customer) outside of the EEA, incorporate the Standard Contractual Clauses or such other mechanism as directed by the Customer into the contract between Supplier and each Subprocessor to ensure the adequate protection of the transferred Customer Personal Data. Alternatively, at Customer's request Supplier shall procure that each Subprocessor enters directly into the Standard Contractual Clauses or such other mechanism with Customer; and

6.2.5 remain fully liable to the Customer for any failure by each Subprocessor to fulfil its obligations in relation to the Processing of any Customer Personal Data.

7. **Data Subject Rights**

7.1 Supplier shall promptly (within three (3) business days) notify the Customer if it receives a request from a Data Subject under any Data Protection Laws in respect of Customer Personal Data.

7.2 Supplier shall co-operate as requested by the Customer to enable the Customer to comply with any exercise of rights by a Data Subject under any Data Protection Laws in respect of Customer Personal Data and comply with any assessment, enquiry, notice or investigation under any Data Protection Laws in respect of Customer Personal Data or this Addendum, which shall include:

7.2.1 the provision of all data requested by the Customer within any reasonable timescale specified by the Customer in each case, including full details and copies of the complaint, communication or request and any Customer Personal Data it holds in relation to a Data Subject;

7.2.2 where applicable, providing such assistance as is reasonably requested by the Customer to enable the Customer to comply with the relevant request within the timescales prescribed by the Data Protection Laws; and

7.2.3 implementing any additional technical and organisational measures as may be reasonably required by the Customer to allow the Customer to respond effectively to relevant complaints, communications or requests.

8. **Personal Data Breach**

8.1 Supplier shall notify the Customer immediately, and in any case within twenty-four (24) hours, upon becoming aware of or reasonably suspecting a Personal Data Breach providing the Customer with sufficient information which allows the Customer to meet any obligations to report a Personal Data Breach under the Data Protection Laws. Such notification shall as a minimum:

8.1.1 describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

8.1.2 communicate the name and contact details of Supplier's data protection officer or other relevant contact from whom more information may be obtained;

8.1.3 describe the likely consequences of the Personal Data Breach; and

8.1.4 describe the measures taken or proposed to be taken to address the Personal Data Breach, and any measures to be taken to reduce the risk of future Personal Data Breaches from occurring.

8.2 Supplier shall co-operate with the Customer and take such reasonable commercial steps as are directed by the Customer to assist in the investigation, mitigation and remediation of each Personal Data Breach.

8.3 In the event of a Personal Data Breach, Supplier shall not inform any third party without first obtaining the Customer's prior written consent, unless notification is required by EU or Member State law to which Supplier is subject, in which case Supplier shall to the extent permitted by such law inform the Customer of that legal requirement, provide a copy of the proposed notification and consider any comments made by the Customer before notifying the Personal Data Breach.

9. **Data Protection Impact Assessment and Prior Consultation**

9.1 Supplier shall provide reasonable assistance to the Customer with any data protection impact assessments which are required under Article 35 GDPR and with any prior consultations to any supervisory authority of the Customer or any Customer Affiliate which are required under Article 36 GDPR, in each case solely in relation to Processing of Customer Personal Data by Supplier on behalf of the Customer and taking into account the nature of the Processing and information available to Supplier.

10. **Deletion or return of Customer Personal Data**

10.1 Subject to section 10.2, Supplier shall promptly and in any event within 90 (ninety) calendar days of the earlier of: (i) cessation of Processing of Customer Personal Data by Supplier; or (ii) termination of the Agreement; at the choice of the Customer (such choice to be notified to Supplier in writing) either:

10.1.1 return a complete copy of all Customer Personal Data to the Customer by secure file transfer in such format as notified by the Customer to the Supplier and securely wipe all other copies of Customer Personal Data Processed by Supplier or any Authorised Subprocessor; or

10.1.2 Securely wipe all copies of Customer Personal Data Processed by Supplier or any Authorised Subprocessor,

and in each case provide written certification to the Customer that it has complied fully with this section 101.

10.2 Notwithstanding section 10.1, Supplier may retain Customer Personal Data to the extent required by Union or Member State law and only to the extent and for such period as required by Union or Member State law and always provided that Supplier shall ensure the confidentiality of all such Customer Personal Data and shall ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the Union or Member State law requiring its storage and for no other purpose.

11. **Audit rights**

11.1 Supplier shall make available to the Customer on request all information necessary to demonstrate compliance with this Addendum and allow for and contribute to audits, including inspections by the Customer or another auditor mandated by the Customer of any premises where the Processing of Customer Personal Data takes place. Supplier shall permit the Customer or another auditor mandated by the Customer to inspect, audit and copy any relevant records, processes and systems in order that the Customer may satisfy itself that the provisions of this Addendum are being complied with. Supplier shall provide full co-operation

to the Customer in respect of any such audit and shall at the request of the Customer, provide the Customer with evidence of compliance with its obligations under this Addendum. Supplier shall immediately inform the Customer if, in its opinion, an instruction pursuant to this section 11 (Audit Rights) infringes the GDPR or other EU or Member State data protection provisions.

12. **International Transfers of Customer Personal Data**

12.1 Supplier shall not Process the Customer Personal Data nor permit any Authorised Subprocessor to Process the Customer Personal Data in a Restricted Country, unless authorised in writing by the Customer and in advance.

12.2 When requested by the Customer, Supplier shall promptly enter into (or procure that any relevant Subprocessor of Supplier enters into) an agreement with the Customer or a Customer Affiliate including the Standard Contractual Clauses and/or such variation as Data Protection Laws might require, in respect of any Processing of Customer Personal Data in a Restricted Country, which terms shall take precedence over those in this Addendum.

13. **Codes of Conduct and Certification**

13.1 Supplier shall at the request of the Customer comply with any Code of Conduct approved pursuant to Article 40 GDPR and obtain any certification approved by Article 42 GDPR from time to time, to the extent that they relate to the Processing of Customer Personal Data.

14. **Indemnity**

14.1 Notwithstanding any limitation or exclusion of liability contained within the Agreement, Supplier shall indemnify and hold harmless the Customer against all costs, damage, losses, fines and sanctions arising from any claim by a third party or Supervisory Authority arising from any breach of this Addendum.

15. **General Terms**

15.1 Subject to section 15.2, the parties agree that this Addendum and the Standard Contractual Clauses shall terminate automatically upon termination of the Agreement (or expiry or termination of all contracts entered into by Supplier with the Customer pursuant to the Agreement, whichever is later).

15.2 Any obligation imposed on Supplier under this Addendum in relation to the Processing of Personal Data shall survive any termination or expiration of this Addendum.

15.3 Supplier is familiar with the applicable Data Protection Laws and is in material compliance with its obligations as a Data Processor.

15.4 Any breach of this Addendum shall constitute a material breach of the Agreement.

15.5 Compliance by Supplier with the provisions of this Addendum will be at no additional cost to the Customer.

15.6 Except to the extent set out section 15.7 and the Standard Contractual Clauses, a person who is not a party to this Addendum shall have no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Addendum.

15.7 A Customer Affiliate may enforce any term of this Addendum which is expressly or implicitly intended to benefit it.

15.8 The rights of the parties to rescind or vary this Addendum are not subject to the consent of any other person.

15.9 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

ANNEX 1: DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

This Annex 1 includes certain details of the Processing of Customer Personal Data as required by Article 28(3) GDPR.

The subject matter and duration of the Processing of the Customer Personal Data are set out in the Agreement which describes the provision of goods and/or services to Customer.

The Personal Data processed under this Addendum may contain the following categories of Personal Data:

i. Personal master data (name, address, title, degree, date of birth);
ii. Contact details (telephone number, mobile phone number, email address, fax number, address data);
iii. Contractual master data;
iv. Client histories;
v. System access / usage / authorisation data;
vi. Personal Data relating to financial information and/or employment relationships;
vii. Personal Data revealing racial or ethnic origin;
viii. Personal Data revealing political opinions;
ix. Personal Data revealing religious or philosophical beliefs;
x. Personal Data revealing trade union membership;
xi. Genetic or biometric data;
xii. Data concerning health;
xiii. Data concerning a natural person's sex life or sexual orientation; and
xiv. Personal Data relating to criminal convictions and offences.

The groups of Data Subjects who's Personal Data are processed under this Addendum may include the following:

Past and present customers; past and present employees; past and present contractors or consultants; agency-supplied contractors or consultants and external secondees; job applicants and candidates; students and volunteers; individuals identified by employees or retirees as beneficiaries, spouse, domestic/civil partner, dependents and emergency contacts; retirees; past and present directors and officers; shareholders; bondholders; account holders; end-users / consumers (adults, children); patients (adults, children); by-passers (CCTV cameras); and website users.

ANNEX 2: TECHNICAL AND ORGANISATIONAL MEASURES

General Comment:

Iron Mountain understands that some of these measures do not apply to the extent the Supplier does not Process Personal Data electronically on its (or its subprocessors') systems or has access to Iron Mountain's systems that process Personal Data.

1.1 Physical Access Control.

Unauthorised persons are prevented from gaining physical access to premises, buildings or rooms where Data Processing systems that process and/or use Personal Data are located.

Measures:

- Supplier protects its assets and facilities using the appropriate means based on a security classification conducted by an internal security department.
- In general, buildings are secured through access control systems (e.g., smart card access system).
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
- Depending on the security classification, buildings, individual areas and surrounding premises may be further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.
- Access rights are granted to authorised persons on an individual basis according to the System and Data Access Control measures (see Section 1.2 and 1.3 below). This also applies to visitor access. Guests and visitors to Supplier buildings must register their names at reception and must be accompanied by authorised Supplier personnel.
- Supplier employees and external personnel must wear their ID cards at all Supplier locations.

1.2 System Access Control.

Data Processing systems used to provide the Supplier Services must be prevented from being used without authorisation.

Measures:

- Multiple authorisation levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Processes are in place to ensure that authorised users have the appropriate authorisation to add, delete, or modify users.
- All users access Supplier's systems with a unique identifier (user ID).
- Supplier has procedures in place to ensure that requested authorisation changes are implemented only in accordance with the guidelines (for example, no rights are granted without authorisation). If a user leaves the company, his or her access rights are revoked.
- Supplier has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalised user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver.

- The company network is protected from the public network by firewalls.
- Supplier uses up–to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations.
- Security patch management is implemented to ensure regular and periodic deployment of relevant security updates.
- Full remote access to Supplier's corporate network and critical infrastructure is protected by strong authentication.

1.3 Data Access Control.

Persons entitled to use Data Processing systems gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorisation in the course of processing, use and storage.

Measures:

- As part of the Supplier Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the Supplier Information Classification standard.
- Access to personal, confidential or sensitive information is granted on a need-to-know basis. In other words, employees or external third parties have access to the information that they require in order to complete their work. Supplier uses authorisation concepts that document how authorisations are assigned and which authorisations are assigned to whom. All personal, confidential, or otherwise sensitive data is protected in accordance with the Supplier security policies and standards. Confidential information must be processed confidentially.
- All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing personal, confidential or other sensitive information are regularly checked. To this end, Supplier conducts internal and external security checks and penetration tests on its IT systems.
- Supplier does not allow the installation of personal software or other software that has not been approved by Supplier.
- An Supplier security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

1.4 Data Transmission Control.

Except as necessary for the provision of the Services in accordance with the relevant service agreement, Personal Data must not be read, copied, modified or removed without authorisation during transfer. Where data carriers are physically transported, adequate measures are implemented at Supplier to ensure the agreed-upon service levels (for example, encryption and lead-lined containers).

- Personal Data transfer over Supplier internal networks are protected in the same manner as any other confidential data according to Supplier Security Policy.
- When data is transferred between Supplier and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant Agreement. This applies to both physical and network based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of Supplier-controlled systems (e.g. data being transmitted outside the firewall of the Supplier Data Centre).

1.5 Data Input Control.

It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from Supplier data processing systems.

Measures:

- Supplier only allows authorised persons to access Personal Data as required in the course of their work.
- Supplier has implemented a logging system for input, modification and deletion, or blocking of Personal Data by Supplier or its subprocessors within Supplier's Products and Services to the fullest extent possible.

1.6 Availability Control.

Personal Data will be protected against accidental or unauthorised destruction or loss.

Measures:

- Supplier employs backup processes and other measures that ensure rapid restoration of business critical systems as and when necessary.
- Supplier uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to ensure power availability.
- Supplier has defined contingency plans as well as business and disaster recovery strategies for the provided Services.
- Emergency processes and systems are regularly tested.

1.7 Data Separation Control.

Personal Data collected for different purposes must be processed separately.

Measures:

- Supplier uses the technical capabilities of the deployed software (for example: multi- tenancy, or separate system landscapes) to achieve data separation among Personal Data originating from multiple customers.
- Customers (including their Affiliates) have access only to their own data.
- If Personal Data is required to handle a support incident from a specific customer, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems.

1.8 Data Integrity Control.

Personal Data will remain intact, complete and current during processing activities.

Measures:

Supplier has implemented a multi-layered defence strategy as a protection against unauthorised modifications.

In particular, Supplier uses the following to implement the control and measure sections described above.

- Firewalls;
- Security Monitoring Centre;
- Antivirus software;

- Backup and recovery;
- External and internal penetration testing;
- Regular external audits to prove security measures.