DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") is supplemental to the Terms and Conditions for the Supply of Services (the "**Agreement**") between Iron Mountain and the Customer.

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 DPA 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.

The following amendments and/or additions to the Agreement are agreed.

BACKGROUND AND PURPOSE

(A) This DPA sets out the terms and conditions for the Processing of the Personal Data by the Processor on behalf of the Customer under the Agreement, pursuant to which the Customer acquires the Services (as defined in the Agreement) from the Processor.

(B) "**Data Protection Regulation**" shall mean the UK GDPR as the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (EU GDPR) which forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419). The UK GDPR is defined in section 3(10) of the Data Protection Act 2018 (DPA 2018), supplemented by section 205(4) and includes the instructions and binding orders issued by the data protection authorities ("**GDPR**").

IT IS AGREED as follows:

1. DEFINITIONS

Any terms not defined in this DPA shall be given the meaning set forth in the Data Protection Regulation.

"**Agreement**" shall mean the agreement(s) between the parties and/or its affiliates under which the Processor provides services to the Customer.

"**Personal Data**" shall only mean the Personal Data that is subject to the Services under the Agreement.

"**Supervisory Authority**" shall mean the Information Commissioner's Office or any other Independent public authority with responsibility for monitoring the application of the Data Protection Regulation.

2. RIGHTS AND RESPONSIBILITIES OF THE CUSTOMER

The Customer shall: (i) Process the Personal Data in compliance with the Data Protection Regulation; (ii) be authorised to give documented instructions to the Processor on the Processing of the Personal Data (including on behalf of any third party entity which is a Controller of the Personal Data), such instructions shall be binding on the Processor unless the completion of the instructions requires the provision of

services under the Agreement and the Customer does not approve the corresponding service fees, or the completion of the Customer's instructions would be contrary to any Sections under this DPA; (iii) compensate the Processor for any fees and/or charges as detailed in the Agreement for Services rendered by the Processor, as a consequence of complying with the requirements of this DPA, unless such costs are specified as being for the Processor's account as part of the Services.

3. RIGHTS AND RESPONSIBILITIES OF THE PROCESSOR

3.1 The Processor shall not use the Personal Data for any purposes other than those specified in the Agreement and this DPA.

3.2 The Processor shall: (i) Process the Personal Data in accordance with prevailing information management industry standards and in compliance with applicable laws and regulations; (ii) Process the Personal Data only in accordance with the documented instructions of the Customer and immediately inform the Customer if, in its opinion, a Customer instruction infringes the Data Protection Regulation or other European Union or Member State data protection provisions; (iii) ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; (iv) to the extent feasible and subject to any applicable fees in the Agreement, assist the Customer in its response to rights exercised by Data Subjects or powers exercised by Supervisory Authorities under the Data Protection Regulation; (v) provide the Customer with all information necessary to demonstrate compliance with the Processor's obligations set out in this DPA and in the Data Protection Regulation; (vi) allow for and contribute to audits, including inspections, conducted by the Customer as set forth (and subject to the limitations) in Section 5 of this DPA; (vi) provide reasonable assistance to the Customer with any data protection impact assessments and with any prior consultations to a Supervisory Authority, in each case where these are required by the Data Protection Regulation, and solely in relation to Processing of Personal Data by the Processor on behalf of the Customer and taking into account the nature of the Processing and information available to the Processor.

3.3 This DPA shall not prevent the Processor from disclosing or otherwise Processing the Personal Data as required by law, regulation or by a competent court or Supervisory Authority.

3.4 If a Supervisory Authority or a competent court makes a request concerning the Personal Data, the Processor shall inform the Customer of such requests without undue delay and prior to any response or other action concerning the Personal Data. If the law or regulation prescribes an immediate response to the Supervisory Authority or a competent court, the Processor shall respond and inform the Customer that it has done so as soon as reasonably possible unless such notice to the Customer is prohibited by the respective law, regulation or warrant. The Processor may only correct, delete, amend or block the Personal Data processed on behalf of the Customer when instructed to do so by a competent court or Supervisory Authority or as required by law or regulation.

Data Security

3.5 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, the Processor shall implement technical and organisational measures to ensure the confidentiality, integrity, availability of the Personal Data and to protect the Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration, or disclosure. Such technical and organisational measures are contained in the Security Assurance Reference Guide of the Processor that can be provided to the Customer upon request.

Personal Data Breach Notification

3.6 In the event of a Personal Data Breach, the Processor shall without undue delay notify the Customer once it has a reasonable degree of certainty that a Personal Data Breach has occurred.

3.7 The Personal Data Breach notification shall contain at least the following (to the extent the Processor is privy to such information): a description of the nature of the Personal Data Breach including, the categories and approximate number of Data Subjects concerned and the categories and approximate number of data records concerned; a description of likely consequences of the Personal Data Breach; and a description of the measures taken to address the Personal Data Breach and to mitigate its possible adverse effects.

3.8 Where, and in so far as, it is not possible to provide the information listed in Section 3.7 at the same time, the information may be provided in phases without undue further delay. In such cases when the Processor cannot provide certain information listed in Section 3.7 to the Customer, the Processor will inform the Customer accordingly.

3.9 The Processor shall take reasonable steps to protect the Personal Data after having become aware of a Personal Data Breach. After having notified the Customer in accordance with the requirements of the Data Protection Regulation, the Processor shall take appropriate measures to secure the Personal Data and limit any possible detrimental effect to the Data Subjects. The Processor will cooperate with the reasonable instructions of the Customer, with any third parties designated by the Customer, and with any Supervisory Authority, to respond to the Personal Data Breach.

Returning or Destruction of Personal Data

3.10 Any Personal Data contained within items stored by the Processor on behalf of the Customer will be returned to the Customer in accordance with an agreed exit plan, and subject to agreed exit costs, as stipulated in the Agreement. In all other cases, the Processor will return the Personal Data to the Customer or to a third party designated by the Customer and/or destroy the Personal Data in accordance with the instructions of the Customer. If the Customer fails to give any instructions regarding the deletion/destruction or return of Personal Data following the termination/expiry of the Agreement, the Customer hereby authorises the Processor to further process all Personal Data even after the termination of the Agreement until such time as the Customer provides the instructions.

3.11 Notwithstanding 3.10, the Processor shall not be in breach of its obligations with respect to the deletion of Personal Data retained on back-up tapes as long as such back-up tapes are overridden (and thereby the Personal Data deleted) in the normal course of business.

4. SUBPROCESSORS AND DATA TRANSFER

4.1 The Customer acknowledges and authorises the Processor to engage the third parties and affiliates ("**Approved Subprocessor"**) to Process the Personal Data that are listed and accessible via www.google.com/url?q=https://www.ironmountain.com/-/media/files/Utility/Legal/EU-Personal-Data-Subprocessors-List.xlsx&sa=D&source=editors&ust=1625675288904000&usg=AOvVaw0HXPgpjbJmJnCBvDikhDBr. If a Subprocessor processes the Personal Data outside the EEA and the recipient country does not provide an adequate level of protection for the Personal Data, the necessary safeguards (such as EU Commission's Standard Contractual Clauses or similar approved mechanisms) that legitimise the data transfer shall also be implemented by the Processor. Documentation about the data transfer mechanism shall be provided to the customer upon request. The authorisation provided by the Customer under this section 4.1 also includes an express authorisation by the Customer to enable the Processor to directly enter into Standard Contractual Clauses with each Subprocessor on behalf of the Customer.

4.2 In case any additions or replacements to the list of Subprocessors are required, the Processor shall notify the Customer by email in advance of such addition or replacement. In order to receive these email notifications, the Customer shall subscribe and manage any existing subscription to Processor's notification mechanism via this web page (https://urldefense.proofpoint.com/v2/url?u=https-3A__reach.ironmountain.com_LegalSubprocessorSubscription&d=DwMFaQ&c=jxhwBfk-KSV6FFIot0PGng&r=JTlzF2zjI-gYEq5GmWmZcbgd--hqyVuIeEIP9Eu7Nvw&m=NB4wIISphmYGgqvrtYNU-28S8AaU6-YibdZ3Yg_2F68&s=xNzeKIzw6XbGZ_loyLbqEap2144HRDTflVtNiXKr6M4&e=). If the Customer fails to subscribe to this notification service, the Processor will be unable to provide notifications to the Customer by other means and shall not be liable for the lack of Subprocessor notification. If the Customer fails to subscribe, Customer will not receive notification of the appointment and all such appointments shall be deemed to be authorised by the Customer. If the Customer subscribes, the appointment of any new Subprocessor shall be deemed authorised by the Customer unless Customer reasonably objects on demonstrable grounds that relate to data protection in writing and within fifteen (15) days of Processor's provision of notice.

4.3 The Processor shall impose contractual terms on its Subprocessors which are no less onerous than those set out in this DPA.

4.4 The Processor shall regularly monitor the performance of its Subprocessors and is fully liable for the Personal Data processing activities of its Subprocessors.

5. AUDITS

The Customer shall have the right to perform audits and inspections of the Processor's and its Sub Processors' facilities in accordance with the Agreement. Except where a Personal Data Breach has occurred, no more than one such audit shall be conducted in any twelve (12) month period.

6. LIABILITY

6.1 In the event of any Personal Data Breach which arises directly from the Processor's illegal, unauthorised or negligent Processing of Personal Data, the Processor agrees to reimburse, to the extent required by law, the Customer on demand for the direct, verifiable, necessary and properly incurred third-party costs of the Customer in: (a) preparation and mailing of notices to such individuals to whom such notification is required by law; and (b) the provision of credit monitoring services to such individuals as required by law for a period not exceeding twelve (12) months; provided that the Customer gives the Processor reasonable prior written notice of its intent to deliver such notice.

6.2 Each party (the "**Indemnifying Party**") agrees to indemnify the other party (the "**Indemnified Party**") from and against any third-party claims from Data Subjects, to the extent that the claim results directly from any act or omission by the Indemnifying Party for a violation of GDPR. The Indemnifying Party shall not be liable for any portion of such claim resulting from (i) Indemnified Party's violation of GDPR, or (ii) claims which otherwise could have been avoided or mitigated through the commercially reasonable efforts of the Indemnified Party. The Indemnified Party shall grant the Indemnifying Party the option to control the defense and/or settlement of the claim or demand and, in the event the Indemnifying Party exercises such option to control the defense/settlement, then (i) the Indemnifying Party shall not settle any claim requiring any admission of fault on the part of the Indemnified Party without its prior written consent, (ii) the Indemnified Party shall have the right to participate at its own expense, in the claim or suit and (iii) the Indemnified Party shall cooperate with the Indemnifying Party as may be reasonably requested. The Indemnifying Party's sole obligation hereunder shall be to pay any judgment rendered, or settlement made, as a result of such claim or demand.

6.3 Where one party has paid full compensation for damage suffered by a Data Subject as a result of an infringement of the GDPR, that party shall be entitled to claim back from the other party involved in the same processing, the part of the compensation corresponding to the other party's responsibility for the damage in accordance with the provisions of Article 82(5) of the GDPR.

6.4 Subject to Sections 6.1, 6 .2 and 6.3 under which each party's liability is uncapped, in no event shall the Processor's liability exceed with respect to Personal Data Breaches, the limits of liability as set out in the Agreement.

6.5 Neither party shall be liable for any fines imposed by a Supervisory Authority on the other party.

7. NOTICES

Notices regarding any dispute, claim or controversy arising out of or relating to this DPA and its appendices, or the breach, termination or validity thereof shall be deemed sufficient if made in accordance with the Agreement.

8. TERM AND TERMINATION

This DPA shall become effective when duly signed by both Parties and shall survive until any of the Customer's Personal Data ceases to be processed by the Processor in accordance with 3.1.9 and 3.1.10.

9. PRIOR AGREEMENTS

This DPA supersedes and replaces any and all previous data processing agreements or data protection or privacy clauses between the Parties.

10. APPLICABLE LAW AND DISPUTE RESOLUTION.

This DPA, and any dispute, claim or controversy arising out of or relating to this DPA, or the breach, termination or validity thereof, are governed by the laws governing the Agreement without regard to its principles and rules on conflict of laws.

11. CHANGES IN DATA PROTECTION LAWS

Each Party may notify the other Party in writing from time to time of any variations to this DPA which the Party reasonably considers to be necessary to address the requirements of the Data Protection Regulation or any decision of a Supervisory Authority or competent court. Any such variations shall take effect thirty (30) calendar days after the date such written notice is sent to the other Party, unless the other Party notifies the Party sending the notice of any reasonable objections within this thirty (30) day period, in which case the Parties shall cooperate in good faith to agree on the form of the variations.

APPENDIX 1

CATEGORIES of PROCESSING ACTIVITIES; PERSONAL DATA and DATA SUBJECTS

The processing activities are set forth in the Agreement as Services.

The Personal Data processed under this DPA shall 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. Customer history;
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 whose Personal Data are processed under this DPA consist of the following: 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.

The Customer will not deliver to the Processor Personal Data outside scope indicated above or shall notify the Processor in writing about any new data type/data subject.