DATA PROCESSING AGREEMENT (GERMANY)

ANTECEDENTS

(A) This Data Processing Agreement ('**DPA**') sets out the terms and conditions for the processing of personal data under the Service Agreement(s) (the '**Agreement**') signed between Iron Mountain and its customer (the '**Customer**'), pursuant to which the Customer acquires certain the services from Iron Mountain and Iron Mountain provides those services to the Customer. This DPA is incorporated into and forms inseparable annex of the Agreement by reference.

(B) Iron Mountain acts as a data processor or sub-processor and the Customer acts as a data controller or as a data processor, the concepts of which are further defined in the data protection laws (the **'Data Protection Regulation'**). Within the meaning of this DPA, Data Protection Regulation shall mean all applicable data protection laws, including but not limited to the General Data Protection Regulation (the "**GDPR**" (2016/679/EU)) and the instructions and binding orders of the data protection authorities. "**Supervisory Authority**" shall mean the local data protection authority or any other regulatory/supervisory authority, governmental body.

1. PURPOSE OF DATA PROCESSING

The purpose of the processing of the personal data by Iron Mountain is the performance of the services pursuant to the Agreement. The types of personal data processed, the categories of data subjects concerned, and the contact details of Iron Mountain's data protection officer are specified in **Appendix 1** of this DPA.

2. CUSTOMER RIGHTS AND OBLIGATIONS

The Customer shall

(i) process the personal data in compliance with the Data Protection Regulation;

(ii) be entitled to give written instructions to Iron Mountain on the processing of personal data. Such instructions shall be binding on Iron Mountain on the condition that if the completion of the instructions requires the provision of services under the Agreement, or result in costs emerging on Iron Mountain's side, Customer shall simultaneously pay the applicable service fees/emerging costs. Iron Mountain will not meet any Customer instructions which are contrary to any Sections of this DPA;

(iii) at all times retain the control and authority over the personal data. If any data subject requested for information on the processing of personal data, requested the correction of the personal data, disputed the legality of data-processing, or otherwise required the termination of data-processing, or the deletion or blocking of personal data, the Customer shall immediately instruct Iron Mountain to take the appropriate measures; and

(iv) inform Iron Mountain of the categories of personal data processed under the Agreement, and the data subjects involved with data-processing. Iron Mountain raises the Customer's attention that it provides the services on the physical forms of Customer's documents/media (Articles, Folders, Boxes, Media, Media Container, etc.), but not directly on the content of these documents/media, so particularly on the personal data contained therein. Given this, it is Customer's responsibility to notify Iron Mountain in writing should the personal data/data subjects involved with data-processing would be other than as listed in **Appendix 1**.

3. IRON MOUNTAIN RIGHTS AND OBLIGATIONS

3.1. Iron Mountain shall

(i) not use personal data for any purposes other than those specified in the Agreement and this DPA;

(ii) process personal data in accordance with the Data Protection Regulation;

(iii) process personal data only in accordance with written instructions from the Customer (taking into account Section 2 (ii)). Iron Mountain shall immediately inform the Customer if, in its opinion, an instruction infringes the Data Protection Regulation. Nonetheless, Iron Mountain emphasizes again that it directly processes the documents/media of the Customer only, so in most cases, Iron Mountain is unable to assess whether the Customer's instruction was legal;

(iv) assist the Customer in its response to meet requests from data subjects;

(v) provide the Customer with all information necessary to demonstrate compliance with Iron Mountain's obligations set out in this DPA and in the Data Protection Regulation;

(vi) allow for and contribute to audits conducted by the Customer as set forth in Section 7 of this DPA;

(vii) process the personal data only during the term of this DPA;

(viii) ensure that its personnel/subcontractors authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.2. This DPA shall not prevent Iron Mountain from processing the Personal Data as required by law, regulation or by a competent court or Supervisory Authority. If any Supervisory Authority or competent court makes such a request, Iron Mountain shall inform the Customer of that legal requirement before processing, or if the authority/court order requires an immediate or short notice response, once possible, unless such notice is prohibited by the Data Protection Regulation or the respective warrant.

Data security

3.3 Iron Mountain shall implement and document reasonable technical and organisational measures to ensure confidentiality, integrity and availability of personal data, and to protect the personal data against unlawful processing. Brief summary of the applied technical and organisational measures are attached hereto as **Appendix 2**.

3.4 Iron Mountain shall periodically test, assess and evaluate the effectiveness of its technical and organisational measures.

Personal Data Breach notification

3.5 In the event of a '**Personal Data Breach**', i.e., a breach of security leading to accidental or unlawful destruction, loss, alternation, unauthorised disclosure of, or access to the personal data, Iron Mountain will without undue delay notify the Customer via e-mail.

3.6 The Personal Data Breach notification shall contain at least the following (to the extent Iron Mountain 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.

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

3.8 Iron Mountain shall document all Personal Data Breaches, and shall have the record available to the Customer upon request.

3.9 Iron Mountain shall take appropriate steps to protect the personal data after having become aware of a Personal Data Breach in order to limit any possible detrimental effect to the data subjects. Iron Mountain will cooperate with the Customer to respond to the Personal Data Breach.

4. RETURNING OR DESTRUCTION OF PERSONAL DATA

4.1 With respect to personal data stored on physical Customer assets, such as Articles and Media, upon termination/expiry of the Agreement, based on Customer's specific instructions, but always subject to Iron Mountain's fees (or any emerging costs) payable by the Customer, Iron Mountain shall either destroy or return to the Customer all such physical assets. If the Customer fails to give any instructions within 15 calendar days of the termination/expiry of the Agreement, Iron Mountain shall send a written notice to the Customer requesting to receive within 15 calendar days specific instructions whether to destroy or to return the assets. Should the Customer fail to provide written instructions within this timeframe, and pay the applicable fees (costs), then the Customer hereby authorises Iron Mountain that, upon its own discretion, further store, delete/destruct or return all these assets even after the termination/expiry of the Agreement.

4.2 With respect to personal data not stored on the physical Customer assets, Iron Mountain shall delete the personal data once the Agreement terminated/expired. Back-up data might be retained on back-up tapes as long as such tapes are overridden.

4.3 Upon Customer's request, Iron Mountain shall confirm to the Customer in writing that the deletion/destroy or return of Personal Data has been accomplished.

5. TRANSFER OF PERSONAL DATA

5.1 Iron Mountain will always keep all physical Customer assets (including Articles/Boxes/Media/Media Containers) within the European Economic Area (EEA). In case of regular RM and Scanning Services, the scanned images taken of the Customer's Articles, as well as the electronically available inventory listings/data related to the stored Customer assets might be kept and processed on IT-systems/servers which are located outside the EEA, in third countries. The Customer consents that the aforementioned, electronically available information will be processed on IT-systems/servers located outside the EEA in the countries listed in **Appendix 3**. The foregoing right is subject to such transfers being under the terms of the EU Commission's Standard Contractual Clauses or similar approved mechanisms. Customer hereby entrusts Iron Mountain to enter into EU Commission's Standard Contractual Clauses on Customer's behalf.

5.2 For any personal data transfer other than in 5.1 (e.g. wider scope of transfer, new country location), Iron Mountain shall inform the Customer in advance. Unless the Customer objects in writing within 15 calendar days of being informed by Iron Mountain to such a transfer, Iron Mountain may process such transfer, provided that the appropriate safeguards (EU Commission's Standard Contractual Clauses, etc.) are in place. If Customer made an objection within the given timeline, Iron Mountain will use reasonable efforts to change its data transfer system or recommend a commercially reasonable change to the Customer's use of the services under the Agreement to avoid transfer of the personal data. If Iron Mountain is unable to make available such a change or if Customer rejects such a change within 60 calendar days, the Customer may terminate within further 60 calendar days from Iron Mountain's notice (or – if Iron Mountain failed to reply – from the expiry of the 60 days available for Iron Mountain's notice) the Agreement. If Customer fails to send such a termination notice to Iron Mountain within this deadline, this shall be considered as consent to transferring the personal data the said way.

6. SUB-PROCESSORS (SUBCONTRACTORS)

6.1 The Customer acknowledges and agrees that (a) Iron Mountain's affiliates or parent companies may be retained as sub-processors; and that (b) Iron Mountain and its' affiliates or parent companies respectively may engage the third-party sub-processors listed in **Appendix 3** to process personal data for the indicated scope of services. Customer understands that Iron Mountain's global sub-processors will only be applied in the RM and Scanning service lines, when the scanned images taken of the Customer's Articles, as well as the electronically available inventory listings/data related to the stored Customer assets are processed by these entities (see Section 5.1).

6.2 In case of any additions or change to the current list, Iron Mountain shall notify the Customer in advance - indicating the name, country location, and subcontracted service of the proposed new sub-processor. Unless Customer objects in writing within 15 calendar days of being informed about Iron Mountain's use of a new sub-processor, Iron Mountain may apply the new sub-processor for the indicated data processing activities. If Customer made an objection within the given timeline, Iron Mountain will use reasonable efforts to change the Services to avoid processing of the personal data by the "objected-to" new sub-processor. If Iron Mountain is unable to implement such changes within 60 calendar days, the Customer within further 60 calendar days from Iron Mountain's notice (or – if Iron Mountain failed to reply – from the expiry of the 60 calendar days available for Iron Mountain's notice) may terminate the Agreement. If Customer fails to send such a termination notice to the Iron Mountain within this deadline, this can be considered as consent to the application of the proposed sub-processor.

6.3 Iron Mountain is obliged to regularly monitor the performance of its subcontractors, and remains responsible for the personal data processing activities of its sub-processors as if the processing activities were carried out by Iron Mountain itself. Iron Mountain imposes the same data protection obligations as set out in this DPA on all its applied sub-processors.

7. AUDITING

Iron Mountain makes available to the Customer all information necessary to demonstrate compliance with the obligations laid down in this DPA, and allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer. However, audit rights under this DPA shall not grant access to any data of other Iron Mountain customers, or to data related to Iron Mountain's applied security systems/measures. Iron Mountain assists the Customer in data protection impact assessments, and prior consultations with the Supervisory Authorities, insofar as such assistance is Iron Mountain's obligation under the Data Protection regulation.

8. TERM AND APPENDICES

This DPA shall become effective when the Agreement is duly signed by both Parties, and shall survive until all of Customer's personal data are either returned to the Customer, or otherwise deleted/destroyed. The Appendices form integral part of this DPA.

***

Appendix 1

Categories of Personal Data and data subjects

The categories of Personal Data processed under the Agreement(s):

☒ name
☒ phone number
☒ nationality, ethnic data
☒ marital status
☒ tax identification data (e.g. tax ID number)
☒ property and income data
☒ work-related data (e.g. job title, workplace)
☒ qualification and study data
☒ IP-address

☒ address, place of residence
☒ e-mail address
☒ date and place of birth
☒ personal identification numbers (e.g. personal ID No.)
☒ salary data (e.g. wage)
☒ data related to creditworthiness
☒ image (e.g. photo)
☒ username, password
☒ individual identification number (e.g. customer ID)

The groups of data subjects whose Personal Data are processed under the Agreement:

☒ employees
☒ customers
☒ insured
☒ patient

☒ subcontractors
☒ suppliers
☒ customers, employees, contact personnel of third parties
☒ applicants

Customer will not deliver to Iron Mountain Personal Data outside the scope indicated above, or shall notify Iron Mountain in writing and in advance about any new data type/data subject concerned.

Contact details of Iron Mountain’s data protection officer:

Attn. Sascha Votteler
IRON MOUNTAIN DEUTSCHLAND GMBH
+49 (0)173 – 94 91 283 – mobile
sascha.votteler@ironmountain.com - email
Iron Mountain Deutschland GmbH, Kanalstr. 119, 12357 Berlin - seat

Appendix 2
Summary of applied technical and organisational measures

1. Process Specifications

1.1 Scope

This Summary applies to the technical and organizational measures applied by Iron Mountain Deutschland GmbH and Iron Mountain (Deutschland) Service GmbH (hereinafter jointly as: Iron Mountain Germany).

1.2 Process Owner

Department: Risk & Compliance

1.3 Responsible Functional Areas

All site managers of Iron Mountain Germany.

2. Purpose

As a service provider in information management Iron Mountain Germany has to implement technical and organizational measures (TOMs) to ensure that the security and protection requirements of the General Data Protection Regulation (GDPR) are met. This document describes the existing / implemented measures of Iron Mountain Germany.

3. Technical and Organizational Measures

3.1 Confidentiality (Article 32 Paragraph 1 (b) GDPR)

3.1.1 Entrance Control

Objective: No unauthorized entrance to data processing systems

Existing / implemented measures:

- Fence system (1) with driveway gate
- Closed operating building units
- Illumination of the property in the dark
- Intrusion Detection System (IDS) with direct connection to security service (24/7/365) and emergency power supply (at least 24 h)
- Access control system through personal transponder / door codes
- Documented key control
- Attendance records
- Company´s and visitor´s badge control
- Data protection obligations for employees
- Data protection guidelines for visitors
- Escort of visitors (external partners)
- Video cameras (CCTV) with recording on motion, data memory 30 days
- Emergency exit doors with day alarm
- Labeling of data processing areas (SISP – Sensitive Storage and Processing Area)
- Additional access controls of sensitive areas (archives, IT rooms)
- Prohibition of image and voice recordings in the SISP areas.

(1) Due to structural conditions and fire brigade driveways no or limited fencing is available in the archive centers Hamburg-Hammerbrook (high-rise bunker), Hamburg-Rahlstedt, Hofheim and Markt Schwaben.

3.1.2 Access Control

Objective: No unauthorized use of system

Existing / implemented measures:

- Approval process for allocating access to IT systems
- IT system access only via personal user IDs
- Time limit of access rights
- Minimum requirements for passwords
- Forced password change at first login
- Disconnection due to incorrect logon attempts
- Automatic screen lock
- IT terms of use and security policy
- Limited use of storage media (USB sticks)
- Encryption during data transfers
- Controlled media destruction by external partners acc. to DIN 66399

3.1.3 Process Control

Objective: No unauthorized reading, copying, modification or removal within the system

Existing / implemented measures:

- Approval process for access authorizations
- Data access only via personal user IDs
- Labeling, capturing and tracking of the data per barcode and barcode scanner
- Authorization and role concepts
- Control of access rights
- Remote access only via secured VPN connection
- External security via firewall systems
- Confidentiality obligation (GDPR / Federal Data Protection Act)
- Order agreements with external partners
- Mobile device management
- Documented logout processes

3.1.4 Separation Control

Objective: Separate processing of data collected for different purposes

Existing / implemented measures:

- Multi-client capable systems and workflows
- Order related service contracts
- Unique identifiers (customer IDs, unique barcodes)
- Purposeful data processing
- Separation of functions for productive and testing data

3.1.5 Pseudonymisation (Article 32 Paragraph 1 (a) GDPR; Article 25 Paragraph 1 GDPR)

Objective: The processing of personal data in such a way that it is no longer possible to assign data to a specific data subject without the need for additional information provided that such additional information is stored separately and subject to appropriate technical and organizational measures.

Existing / implemented measures:

- Purpose limitation according to customer agreements
- Data encryption (not applicable to data contained on hard-copy documents)
- Customer IDs
- Anonymous archiving cartons, an assignment to client or content from the outside is not possible
- Coded archive units
- Coded locations
- Principle of chaotic storage

3.2 Integrity (Article 32 Paragraph 1 (b) GDPR)

3.2.1 Disclosure Control

Objective: No unauthorized reading, copying, modification or removal during electronic transfer or transportation

Existing / implemented measures:

- Physical separation of loading area and cab
- Alarm system for vehicles
- Automated door locking
- Door opening only after alarm deactivation by transponder
- Starting engine only possible when doors locked
- Immobilizer
- Packing and shipping regulations
- Logged deliveries (delivery note)
- Transfers according to order
- Logging functions
- Information classification
- Clear desk policy

3.2.2 Data Entry Control

Objective: Identification whether and by whom personal data is entered, altered or removed in data processing systems

Existing / implemented measures:

- Order related service contracts

- Responsibility rules
- Process flow organization
- Logging functions (input, change)
- Document management system

3.3 Availability and Resilience (Article 32 Paragraph 1 (b) GDPR)

3.3.1 Availability Control

Objective: Protection against accidental or willful destruction or loss

Existing / implemented measures:

- Structural and organizational fire protection
- Fire alarm systems
- Smoke and heat exhaust ventilation systems (SHEVS)
- Separate fire sections
- Hand fire extinguishers
- Fire safety training and clearance
- No smoking in the buildings
- Sprinkler extinguishing systems (2) for box or file storage (records management)
- External partner to manage water damage
- Early smoke detection (3) (VESDA)
- Gas extinguishing system (4) for data storage
- Incident processes
- Firewall systems
- Antivirus programs
- Backups
- Temperature and humidity recording
- Pest control

(2) Due to structural conditions / restrictions no sprinkler extinguishing system is available for records management in the archive centers Bochow, Damsdorf and Markt-Schwaben.
(3) Early detection of flue gas is available only in the archive centers Berlin, Bochow, Bochum, Butzbach, Hofheim, Münster, Fürstenfeldbruck and Wipshausen.
(4) Due to structural conditions / restrictions no gas extinguishing system is available for data carrier storage in the archive centers Damsdorf and Markt Schwaben.

3.3.2 Rapid Recovery (Article 32 Paragraph 1 (c) GDPR)

Objective: To be able to quickly restore the availability and access of personal data in the event of a physical or technical incident

Existing / implemented measures:

- Crisis management
- Risk management
- Emergency plans and drills
- Emergeny reporting channels
- Recovery processes
- Defined downtime
- Recovery plans

3.4 Procedure for regular review, assessment and evaluation (Article 32 Paragraph 1 (d) GDPR; Article 25 Paragraph 1 GDPR)

3.4.1 Data Protection Management

Objective: Demonstrable compliance with data protection and data protection regulations

Existing / implemented measures:

- Privacy policy
- Privacy trainings
- Data protection obligation for employees
- Data protection guidelines for visitors and external partners
- Certificates of conduct of the employees without entries, annual update
- Involvement of the internal data protection officer
- Reporting process in case of data breaches
- Order data agreement
- IT terms of use and security policy
- Compliance hotline

3.4.2 Incident Response Management

Existing / implemented measures:

- Incident definitions
- Incident reporting processes
- Incident documentation
- International incident reporting
- Crisis management

3.4.3 Privacy by Default (Article 25 Paragraph 2 GDPR)

Objective: Appropriate technical and organizational measures to ensure that, by default, only personal data is processed, which processing purpose is absolutely necessary. This applies to the amount of personal data collected, the extent of its processing, the period of its storage and its accessibility.

Existing / implemented measures:

- Purpose limitation through contracts (specifications of the customer)
- Authorization concepts
- Contractually agreed retention period

3.4.4 Order Control

Objective: No data processing by order within the meaning of Article 28 GDPR without corresponding instruction of the client

Existing / implemented measures:

- Clear contract design
- Change management
- Documented procedures
- Trained employees
- Internal audits
- Supplier management

***

Appendix 3 (List of sub-processors)

GLOBAL SUB-PROCESSORS	APPLIED SERVICE LINE	PROVIDED SERVICE	COUNTRY	APPLIED SAFEGUARDS
Iron Mountain UK PLC Ground Floor, 4 More London Riverside, London SE1 2AU, UK	RM, DP, Scanning	IT support	UK	Model Clauses
HCL Technologies Limited/ HCL America Incorporated Technology Hub, SEZ, Plot No. 3A, Sector 126, Noida – 201304, India 330 Potrero Ave, Sunnyvale, California 94085, USA	RM, Scanning	IT support	India/USA	Model Clauses
Iron Mountain Information Management LLC / Iron Mountain Incorporated / Iron Mountain Intellectual Property Management, Inc. One Federal Street, Boston, MA 02110, USA	RM, Scanning	IT support	USA	Model Clauses
Iron Mountain Services Private Limited Level 02, Block A, WTC-2, Bagmane World Technology Centre (BWTC)	RM, Scanning	IT support	India	Model Clauses

LOCAL SUBPROCESSORS			
COMPANY NAME	APPLIED SERVICE LINE	SEAT	PROVIDED SERVICE
Iron Mountain (Deutschland) Service GmbH	RM, DP, Scanning	Randstr.11, 22525 Hamburg, Deutschland	Operational support
Ulshöfer IT GmbH + Co KG	Scanning	Raiffeisenstr. 17, 61191 Rosbach, Deutschland	Operational support
MAMMUT Deutschland GmbH & Co. KG	RM, Scanning	Bergstedter Chaussee 92, 22395 Hamburg, Deutschland	Destruction according to DIN 66399
TES-AMM Central Europe GmbH	DP, SITAD	Blitzkuhlenstraße 169, 45659 Recklinghausen, Deutschland	Deletion (NIST 800-88) or destruction (DIN 66399) of Media