DATA PROCESSING AGREEMENT (FINLAND)

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) 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.

(C) 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 Regulation**. Within the meaning of this DPA, Data Protection Regulation shall mean the General Data Protection Regulation (the "**GDPR**" (2016/679/EU)) including the implementing local laws, instructions and binding orders issued by the **Supervisory Authorities**. Supervisory Authority shall mean the local Data Protection Authority and 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 documented instructions to Iron Mountain on the processing of personal data (including on behalf of any third party entity which is a controller of the personal data). Such instructions shall be binding on Iron Mountain unless the completion of the instructions would require the provision of any existing or new services under the Agreement, and the Customer does not pay/approve the corresponding service fees, or the completion of instructions would be contrary to any Sections of this DPA.

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 and with prevailing information management industry standards; (iii) process personal data in accordance with documented instructions from the Customer (taking into account Section 2 (ii)), and immediately inform the Customer if, in its opinion, an instruction infringes the Data Protection Regulation, (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, (v) subject to any applicable fees in the Agreement, assist the Customer in its response to powers exercised by Supervisory Authorities under the Data Protection Regulation; (vi) 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; (vii) 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; (viii) ensure that its personnel/subcontractors authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, (ix) 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 Iron Mountain on behalf of the Customer, and taking into account the nature of the processing and information available to Iron Mountain.

3.2. This DPA shall not prevent Iron Mountain from disclosing or otherwise 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 a request concerning the personal data, Iron Mountain shall, without undue delay, inform the Customer of such requests prior to any response or other action concerning the personal data, or as soon as possible in case any law or regulation prescribes an immediate response to the Supervisory Authority or a competent court, unless such notice is prohibited by the respective law, regulation or warrant.

Data security

3.3 Iron Mountain shall implement reasonable technical and organisational measures to ensure confidentiality, integrity and availability of personal data, and to protect the personal data against unauthorised or unlawful processing, and against accidental loss, destruction, damage, alteration, or disclosure. Brief summary of the applied technical and organisational measures are attached hereto as **Appendix 2**. Detailed technical and organisational measures are contained in Iron Mountain's Security Assurance Reference Guide that can be provided to the Customer upon request.

Personal Data Breach notification

3.4 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, once it has a reasonable degree of certainty that a Personal Data Breach has occurred.

3.5 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, 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

3.6 With respect to personal data stored on physical Customer assets, such as Articles or Media, based on Customer's specific instructions, but always subject to agreed destruction/withdrawal fees, 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, and pay the agreed fees, the Customer hereby authorises Iron Mountain that, upon its own discretion, further store, delete/destruct or return all these assets after the termination/expiry of the Agreement.

3.7 With respect to personal data not stored on the physical Customer assets, Iron Mountain shall delete the personal data once the Agreement is terminated/expired, unless the Customer instructs Iron Mountain otherwise, within 15 calendar days of the termination/expiration of the Agreement. Back-up data might be retained on back-up tapes as long as such tapes are overridden in the normal course of business.

3.8 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.

4. SUBPROCESSORS AND DATA TRANSFER

4.1 The Customer acknowledges and authorizes Iron Mountain to engage the third parties and affiliates ("**Subprocessor"**) to process the personal data that are listed and accessible under this web address. If a Subprocessor processes 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 legitimize the data transfer shall also be implemented by Iron Mountain. Documentation about the data transfer mechanism shall be provided to the Customer upon request. Such data transfer is considered approved by the Customer. The authorisation provided by the Customer under this section 4.1 also includes an express authorisation by the Customer to enable Iron Mountain 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, Iron Mountain 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 Iron Mountain's notification mechanism via this web page. If the Customer fails to subscribe to this notification service, Iron Mountain 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 authorized by the Customer. If the Customer subscribes, the appointment of any new Subprocessor shall be deemed authorized by the Customer unless Customer reasonably objects on demonstrable grounds that relate to data protection in writing and within fifteen (15) days of Iron Mountain's provision of notice.

4.3 Iron Mountain shall (i) impose contractual terms on its Subprocessors which are no less onerous than those set out in this DPA, (ii) regularly monitor the performance of its Subprocessors.

5. AUDITING

The Customer shall have the right to perform audits and inspections of Iron Mountain's and it's Subprocessors' 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 Iron Mountain's illegal, unauthorised or negligent processing of personal data, Iron Mountain 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 Iron Mountain 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 Iron Mountain's liability exceed with respect to Personal Data Breaches, the limits of liability as set out in the Agreement. Iron Mountain will not be required to reimburse the Customer for Personal Data Breach notification costs with respect to incidents involving Personal Data that are required to be encrypted by law, regulation or prevailing industry standards.

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

7. TERM, PRIOR AGREEMENTS, APPENDICES AND CHANGES IN DATA PROTECTION LAWS

7.1 This DPA shall become effective when the Agreement is duly signed by both Parties, and shall survive until any of the Customer's personal data ceases to be processed by Iron Mountain in accordance with Sections 3.6 and 3.7. This DPA supersedes and replaces any and all previous data processing agreements or data protection or privacy clauses between the Parties. The Appendices form integral part of this DPA.

7.2 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 Personal Data and data subjects

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

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 the Agreement:

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 / customers (adults, children); patients (adults, children); by-passers (CCTV cameras); and website users.

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.

Contact details of Iron Mountain's data protection officer:

Attn. Iron Mountain Data Protection Office
Global.privacy@ironmountain.com
Iron Mountain Europe
Czuczor utca 10, 5th floor
1093 Budapest
HUNGARY

Appendix 2
Summary of applied technical and organisational measures

Iron Mountain is a global company with high focus on security and safety. Iron Mountain applies the following basic technical and organisational measures at its Vantaa 1 and 2 facilities:

Fire protection

- Sprinkle system, alarm on sprinkle system connected to Fire Department and monitored 24/7/365
- Thermal scan- control hot spot on electric board is conducted annual
- Monthly connection test of the fire alarm
- Fire Extinguishers at site
- Yearly Fire safety awareness training.
- Battery charging areas, free from combustible 1.5 meters, and sufficient ventilation to minimise gas build-up.
- Buildings construction is concrete material.
- Written evacuation plan posted at wall.
- Maintains program on fire protection system

Security

- Automatic Access Control Standard, access control on doors by dual principle, card/tag and personal pin code.
- Intruder alarm monitored 24/7/365 by Guard Company.
- Closed Circuit Television, CCTV. Recording 90 days.
- Maintains program in place for AACS, intruder alarm system and CCTV
- Vehicle Security, Vehicle has high security equipment installed in Vans transporting customer material.

SSHE standards (safety, security, health and environmental)

Facility Inspection Standard, Facility inspection conducted every month and cover

- ✓ Security
- ✓ Fire protection
- ✓ Safety risk

Emergency Response standard

- ✓ Fire drills
- ✓ Education/training
- ✓ Business continue plans and training

Incident Investigation Standard
All incidents are reported in a global workflow incident system.

- ✓ Report
- ✓ Investigate
- ✓ Corrective actions
- ✓ Review
- ✓ Close.

Driving Standard, Rules on roads, training program for all couriers.

- ✓ Follow traffic rules
- ✓ Daily vehicle checks.

Powered Industrial Lift Truck standard

- ✓ Daily control of fork lifts
- ✓ Driving license check/control

Other components in SSHE program:

- ✓ Machinery Standard
- ✓ Working at Height Standard
- ✓ First-Aid Standard
- ✓ PPE Standard (PPE is personal protection equipment)
- ✓ Manual Handling Standard, Ergonomic and right way to work, lifting etc.