LENS SPACES DATA PROCESSING AGREEMENT
Effective as of: October 28, 2021

This Lens Spaces Data Processing Agreement ("**DPA**") is entered into by and between Mirantis, Inc., a Delaware corporation, with offices at 900 E. Hamilton Ave., Suite 650, Campbell, CA 95008, USA ("**Mirantis**") and the Customer who accepted the Lens Spaces Terms of Service available at https://www.mirantis.com/company/agreements/ or otherwise entered into an agreement with Mirantis based on which Mirantis makes available to the Customer the Lens Spaces services, as updated from time to time, between Customer and Mirantis (the "**Agreement**").

1. Definitions

The following capitalized terms shall have the following meanings in this DPA:

"**Applicable Data Protection Laws**" means all laws and regulations, applicable to the Processing of Personal Data under the Agreement as amended from time to time, including (but not limited to) laws and regulations of the European Economic Area, Switzerland, the United Kingdom and the United States and its states.

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.

"Customer" means the individual or legal entity that entered into the Agreement referring to this DPA.

"Customer Account Data" means information about the Customer provided to Mirantis in relation to the creation and administration of the Customer's account (such as profile information or contact information).

"Data Subject" means the identified or identifiable person to whom Personal Data relates.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"EEA" or **"European Economic Area"** means the member states of the European Union, Iceland, Liechtenstein and Norway.

"GDPR" means the 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 (General Data Protection Regulation).

"Personal Data" means any information within the User Content relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable household or a legal entity (where such information is protected similarly as personal data or personally identifiable information under Applicable Data Protection Laws).

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" means the entity which Processes Personal Data on behalf of a Controller, including as applicable any "service provider" as that term is defined by the CCPA or similar terms under another Applicable Data Protection Laws.

"**Security Incident**" means a breach of Mirantis' security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to User Content.

"Sensitive Personal Data" means (i) Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited and (ii) Personal Data relating to criminal convictions and offences of Data Subjects.

"Services" means the services provided by Mirantis to the Customer under the Agreement.

"Standard Contractual Clauses" means the clauses adopted by Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, and/or UK Standard Contractual Clauses.

"Third Country" means a country outside the EEA not recognized by the European Commission as providing an

adequate level of protection for Personal Data.

"UK Standard Contractual Clauses" means the Standard Contractual Clauses for data controller to data processor transfers approved by the European Commission in decision 2010/87/EU.

"User Content" means the User Content as defined in the Agreement.

2. Controller and Processor.

For Personal Data contained in the User Content, Customer is the Controller or the Processor processing the data on behalf of another Controller and Mirantis will be the Processor with respect to such data.

3. Data Processing.

3.1 **Scope of Processing.** This DPA applies when Customer uploads or submits User Content through the Services that is qualified as Personal Data under the relevant Applicable Data Protection Laws.

3.2 **Subject matter.** The subject matter of the Processing under this DPA is Personal Data contained in User Content.

3.3 **Duration.** Duration of the data processing of Personal Data under this DPA is determined by Customer's decision to store Personal Data within the Services.

3.4 **Purpose.** The purpose of the data processing under this DPA is the provision of the Services under the Agreement.

3.5 **Nature of the processing:** Storage of Personal Data included in User Content and further operations initiated by Customer from time to time or allowed by the Services features.

3.6 **Categories of Personal Data:** Any category of Personal Data uploaded to the Services by Customer under Customer's account.

3.7 **Categories of Data Subjects:** Any category of data subjects whose Personal Data is uploaded to the Services by Customer under Customer's account.

4. Customer Instructions.

The parties agree that this DPA and the Agreement constitute Customer's documented instructions regarding Mirantis' processing of Personal Data together with the provision of instructions through the features and settings of the Services made available by Mirantis ("**Documented Instructions**"). Mirantis will process Personal Data only in accordance with Documented Instructions of the Customer and/or other Controller, where Customer is not the Controller. Additional instructions outside the scope of the Documented Instructions (if any) require a prior written agreement between Mirantis and Customer. Mirantis agrees and certifies that Mirantis will not: (i) retain, use, or disclose Personal Data except for other purpose that as allowed in the Agreement, this DPA or Applicable Data Protection Laws (including for other commercial purposes than providing services under the Agreement or retaining, using, or disclosing the information outside the relationship between the parties, unless agreed otherwise); or (b) sell Personal Data.

5. Compliance with Applicable Data Protection Laws.

Each party will comply with all Applicable Data Protection Laws applicable to it and binding on it in the performance of this DPA, including the GDPR, CCPA or similar regulations. Customer warrants that it has all necessary consents or other legal titles to upload and process the Personal Data as the User Content into the services and complied with all other legal obligations necessary to transfer the Personal Data into Services.

6. Confidentiality of Customer Data.

Mirantis will not access or use, or disclose to any third party, any Personal Data, except, in each case, (i) as necessary to maintain or provide the Services, or (ii) as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order), or (iii) as determined by Customer through a feature of the Service or other Documented Instructions. When Mirantis is required to disclose User Content to a governmental body, then Mirantis will attempt to redirect the governmental body to request the data directly from the Customer or the Controller. If compelled to disclose Customer Data to a governmental body, then Mirantis will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Mirantis is legally prohibited from doing so.

7. Confidentiality Obligations of Mirantis Personnel.

Mirantis shall make the Personal Data available only to the personnel bound by appropriate contractual or equivalent legal obligation of confidentiality.

8. Security of Data Processing.

8.1 Mirantis has implemented and will maintain the technical and organizational measures for the Services whose minimum standards are described in Annex 1 to this DPA. Customer acknowledges that it has reviewed the technical and organizational measures and, with regards to the type of Personal Data to be processed by the Services, Customer consider such technical and organizational measures appropriate in the context of transferred Personal Data.

8.2 Customer can elect to implement on its own costs additional technical and organizational measures in relation to Personal Data which will meet the adequate level of protection when the measures described in Annex 1 when necessary, taking into account all circumstances of Data Processing. Such technical and organizational measures may include:

8.2.1 pseudonymization and encryption to ensure an appropriate level of security;

8.2.2 measures to allow Customer to backup and archive appropriately in order to restore availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

8.2.3 processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by Customer.

9. No Processing of Sensitive Personal Data.

Customer acknowledges that the Services are not designed for processing of Sensitive Personal Data on behalf of the Customer and agrees that it will not upload or submit any User Content that would contain Sensitive Personal Data to the Services.

10. EEA, UK and Switzerland Specific Terms.

To the extent Personal Data is subject to Applicable Data Protection Laws of a country from the European Economic Area, the United Kingdom or Switzerland, the following additional terms of this Section 10 shall apply:

10.1 Sub-processing.

10.1.1 **Authorized Sub-processors.** Customer generally authorizes Mirantis to use its affiliates and other sub-processors to fulfill its contractual obligations under this DPA or to provide certain services on its behalf ("**Sub-processors**") that are listed at http:/mirantis.com/company/affiliates-and-subcontractors.

10.1.2 **Change of Sub-processors.** At least 15 days before Mirantis engages any new Sub-processor to carry out processing activities on Personal Data on behalf of Customer, Mirantis will update the list and notify Customer about the changes through a mechanism to obtain notice about the intended change to email address registered by Customer. When Mirantis offers such mechanism, Customer agrees to register its email address to which it wishes to receive the notifications as a precondition for delivery of such information by Mirantis. Unless such mechanism is available, Mirantis will provide the notice by another appropriate manner.

10.1.3 **Objections.** If Customer reasonably objects to a new Sub-processor and written Customer's objection is not resolved to Customer's reasonable satisfaction, then Customer has the ability to object the Processing by a new Sub-processor by (i) removing the Personal Data from the Customer Content in order to avoid further Processing by the new Sub-processor or (ii) terminating the Agreement by delivering Mirantis a termination notice with respect to the Agreement.

10.1.4 **Sub-processor Obligations.** Where Mirantis uses any Sub-processor as described in this Section 10:

(i) Mirantis will restrict the Sub-processor's access to Personal Data only to what is necessary to maintain the Services or to provide the Services to Customer;

(ii) Mirantis will enter into a written agreement with the Sub-processor and, to the extent that the Sub-processor performs the same data processing services that are being provided by Mirantis under this DPA, Mirantis will impose on the Sub-processor substantially the same contractual obligations that Mirantis has under this DPA; and

(iii) Mirantis will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processors that cause Mirantis to breach any of Mirantis'

obligations under this DPA.

10.2 Security Incident Notification.

10.2.1 **Security Incident.** Mirantis will (a) notify Customer of a Security Incident without undue delay after becoming aware of the Security Incident, and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

10.2.2 **Mirantis Assistance.** To assist Customer in relation to any Personal Data breach notifications Customer is required to make under the Applicable Data Protection Laws, Mirantis will include in the notification under section 10.2.1 such information about the Security Incident as Mirantis is reasonably able to disclose to Customer, taking into account the nature of the Services, the information available to Mirantis, and any restrictions on disclosing the information, such as confidentiality. Taking into account the nature of the processing, Customer agrees that it is best able to determine the likely consequences of a Security Incident.

10.2.3 **Unsuccessful Security Incidents.** Customer agrees that:

(i) an unsuccessful Security Incident will not be subject to this Section 10.2. An unsusccessful Security Incident is one that results in no unauthorized access to Customer Data or to any of Mirantis' or its subcontractors' equipment or facilities storing Customer Data, and could include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents; and

(ii) Mirantis' obligation to report or respond to a Security Incident under this Section 10 is not and will not be construed as an acknowledgement by Mirantis of any fault or liability of Mirantis with respect to the Security Incident.

10.2.4 **Communication.** Notification(s) of Security Incidents, if any, will be delivered to the Customer by any means Mirantis selects, including via notifications displayed in the Services or by an email. It is Customer's sole responsibility to maintain accurate contact information within the Customer's account accurate.

10.3 Assessments and Documentation.

Taking into account the nature of the Services and the information available to Mirantis, Mirantis will assist Customer in complying with Customer's obligations in respect of data protection impact assessments and prior consultation pursuant to Articles 35 and 36 of the GDPR (or equivalent provisions of other Applicable Data Protection Laws) or other assessments under Standard Contractual Clauses, by providing the information regarding the Services that are not generally available to the Customer. Mirantis' assistance under this Section can be provided as a separate service and subject to a reasonable compensation of the actual effort spent by Mirantis on such a service. The parties agree that where the GDPR or Standard Contractual Clauses require from the parties a documentation of any assessments related to transfer of Personal Data, taking into account the fact that Customer decides which data will be processed, Customer will keep the documentation of the necessary assessments and make it available to the competent supervisory authorities when requested.

10.4 Provision of Information and Audits.

Mirantis shall make available to Customer all information necessary to demonstrate compliance with the obligations under Article 28 of the GDPR or Standard Contractual Clauses and allow for and contribute to the audits and inspections as described further. Mirantis and its subcontractors are audited by an external third party at least as stated in Annex 1. To the extent that Mirantis is audited by such an independent auditor, Customer chooses to mandate such auditor to carry out the audit and inspection over Mirantis instead of Customer. Customer may ask for additional audits or inspections (i) when it proves that the information made available by Mirantis or the third-party auditor is not sufficient to demonstrate compliance with the obligations set out in this DPA, or (ii) Customer received a notification of a Security Incident, or (iii) such auditor inspection is required by Data Protection Laws or by a competent supervisory authority. Mirantis may allow for such additional audits or inspections subject to a prior agreement on the scope of such additional audit, security measures and reasonable compensation of Mirantis resources assisting the Customer with such audit. The parties agreed that any audit or inspection under the Standard Contractual Clauses shall be caried out according to this Section 10.4.

10.5 Transfers of Personal Data from EEA, Switzerland and United Kingdom.

10.5.1 **Additional Terms for Transfers outside EEA and Switzerland.** If, in the performance of the Services, Personal Data that is subject to the GDPR is transferred to a Third Country, then the Parties shall comply with the Standard Contractual Clauses as set out in the Annex 2. Where Customer is the Controller of the Personal Data, the Standard Contractual Clauses with sections applicable for Module Two shall apply. Where Customer is the Processor acting on behalf of a third-party Controller, the Standard Contractual Clauses with sections applicable for Module Three shall apply.

10.5.2 **Additional Terms for Transfers outside United Kingdom.** If, in the performance of the Services, Personal Data that is subject to the Applicable Data Protection Laws of the United Kingdom is transferred to a Third Country, the parties agree that the UK Standard Contractual Clauses shall apply to such transfers taking together with the security measures described in Annex 1 and details of transfers described in Annex 2. The governing law for this purpose will be the laws of England and Wales and any disputes will be resolved by the courts of England and Wales.

10.5.3 **Interpretation of Standard Contractual Clauses for transfers outside United Kingdom and Switzerland.**

In case of any transfers of Personal Data from the United Kingdom subject exclusively to Applicable Data Protection Laws of the United Kingdom ("**UK Data Protection Laws**") and/or transfers of Personal Data from Switzerland subject exclusively to Applicable Data Protection Laws of Switzerland ("**Swiss Data Protection Laws**"), (i) general and specific references in the Standard Contractual Clauses to GDPR or EU or Member State Law shall have the same meaning as the equivalent reference in the UK Data Protection Laws or Swiss Data Protection Laws, as applicable; and (ii) any other obligation in the Standard Contractual Clauses determined by the Member State in which the data exporter or Data Subject is established shall refer to an obligation under UK Data Protection Laws or Swiss Data Protection Laws, as applicable, and (iii) references to EU authorities shall be replaced by references to the competent data protection authority of the United Kingdom or Switzerland, as applicable. In respect of data transfers governed by Swiss Data Protection Laws, the Standard Contractual Clauses also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity.

11. Data Subject Rights

Taking into account the nature of the Services, Mirantis offers Customer with such functionality that Customer may elect to use to comply with its obligations towards data subjects. Should a data subject contact Mirantis with regard to correction or deletion of its Personal Data, Mirantis will use commercially reasonable efforts to forward such requests to Customer. Taking into account the nature of the processing, Customer agrees that it is unlikely that Mirantis would become aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated. Nonetheless, if Mirantis becomes aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated, it will inform Customer without undue delay. Mirantis will cooperate with Customer to erase or rectify inaccurate or outdated Customer Data transferred under the Standard Contractual Clauses by providing technical features that Customer can use to erase or rectify Customer Data.

12. Termination of the DPA.

This DPA shall continue in force until the termination of the Agreement (the "**Termination Date**").

13. Return or Deletion of Customer Data.

The Services provide Customer with controls that Customer may use to retrieve or delete User Content including Personal Data. Up to the Termination Date, Customer will continue to have the ability to retrieve or delete User Content including Personal Data in accordance with this Section. For 90 days following the Termination Date, Customer may retrieve or delete any remaining User Content including Personal Data from the Services, subject to the terms and conditions set out in the Agreement, unless prohibited by law or the order of a governmental or regulatory body or it could subject Mirantis or its Affiliates to liability. After the expiry of this period Mirantis will remove all the User Content including Personal Data as described in the Agreement. The parties agree that any certification of deletion of data pursuant to Standard Contractual Clauses will be provided only upon Customer's written request.

14. Liability

The liability of Mirantis arising out of or related to this DPA whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement. For the avoidance of doubt, Mirantis' total

liability for all claims from Customer arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement.

15. Entire Agreement; Conflict.

Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between any other agreement between the parties including the Agreement and this DPA, the terms of this DPA will control, except that the Service Terms will control over this DPA. Nothing in the DPA shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses.

16. Governing Law.

This DPA shall be governed by the law that is governing for the Agreement and any disputes from this DPA shall be resolved by the courts that are agreed as competent to resolve the disputes from the Agreement. However, where the Standard Contractual Clauses apply, this DPA will be governed by the law and any disputes will be resolved by the courts agreed in the Standard Contractual Clauses.

Exhibit 1

Technical and Organizational Security Measures (Lens Spaces)

1. **Information Security Program.** Mirantis maintains an information security program designed to (a) help Customer secure User Content including Personal Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to Mirantis systems, and (c) minimize security risks, including through risk assessment and regular testing. Coordination of information security objectives is ensured by dedicated person (CISO). The information security program will include the following measures:

   1.1 Systems Security. The systems dedicated for the provision of Services will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. Mirantis ensures access controls and policies to manage what access is allowed to the systems, including the use of firewalls or functionally equivalent technology and authentication controls.

   1.2 Physical Security

   1.2.1 Physical Access Controls. Physical components of the system where Services are hosted are housed in nondescript facilities (the "**Facilities**"). Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Persons with access to the system are assigned photo-ID badges that must be worn while the persons are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.

   1.2.2 Limited Employee and Contractor Access. The access to the Facilities is provided only to those persons who have a legitimate business need for such access privileges. When a person no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked.

   1.2.3 Physical Security Protections. All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. Electronic intrusion detection systems designed to detect unauthorized access to the Facilities are maintained by the provider of the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by individuals is logged and routinely audited.

   1.2.4 Continued Evaluation. Provider of hosting Facilities will conduct periodic reviews of the security of its Facilities and adequacy of its information security program as measured against industry security standards and its policies and procedures.

   1.3 Security Roles and Responsibilities. All Mirantis personnel with access to User Content are subject to confidentiality obligations and regular security trainings.

   1.4 Measures for Ensuring Ongoing Integrity, availability and resilience of processing systems and services. Methodology follows Mirantis Secure Development Lifecycle: plan, develop, validate, operate, launch, monitor. Risks are identified with threat modelling and then mitigated. In testing, security issues can be found and mitigated. By monitoring the system, security problems can be identified and mitigated.

   1.5 Restoration of Availability. Daily backups of data are captured. There's a process in place to restore the system from the backup.

   1.6 Protection of Data During Transmission. Data is transmitted using TLS.

   1.7 Protection of Data During Storage. Data is encrypted at rest using AWS RDS functionality.

   1.8 Events logging. Events logging is incorporated into the system code and into system components provided by AWS. Event logs are collected in AWS Cloudwatch.

   1.9 Measures for Ensuring System Configuration. System is deployed using an "infrastructure as code" approach where the configuration is kept in source control and reviewed before changes.

2. Mirantis Information Security Audits and Certifications

2.1 Testing, Assessing and Evaluating of Effectiveness of Security Measures. Mirantis organizes regular security reviews and penetration tests to evaluate technical and operational security measures. The effectiveness of organizational measures is evaluated annually as part of ISO 27001 compliance.

2.2 ISO 27001 Audits and Certification. Mirantis uses external auditors to verify the adequacy of its security measures. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; (c) will be performed by independent third-party security professionals at Mirantis selection and expense. In addition to the information contained in this DPA, upon Customer's request, and provided that the parties have an applicable NDA in place, Mirantis will make the certificates issued in relation to the ISO 27001 certification available to the Customer.

Exhibit 2

STANDARD CONTRACTUAL CLAUSES
for "Controller-to-Processor" and "Processor-to-Processor" Transfers under the
LENS SPACES DATA PROCESSING AGREEMENT

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of27 April 2016 on the protection of natural persons with regard to the processing of personaldata and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integralpart of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU)2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to addor update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add otherclauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those termsshall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU)2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligationsprovided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Not used

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
[MODULE TWO: Transfer Controller to Processor]

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 ***Instructions***

(a) The data importer shall process the personal data only on documented instructions from thedata exporter. The data exporter may give such instructions throughout the duration of thecontract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 ***Purpose limitation***

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 ***Transparency***

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completedby the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing acopy, but shall provide a meaningful summary where the data subject would otherwise not be able tounderstand the its content or exercise his/her rights. On request, the

Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 ***Accuracy***

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 ***Duration of processing and erasure or return of data***

Processing by the data importer shall only take place for the duration specified in Annex I.B. After theend of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 ***Security of processing***

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personaldata to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. Thedata importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of thecontract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation ofconfidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to addressthe breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Suchnotification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account thenature of processing and the information available to the data importer.

8.7 ***Sensitive data***

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religiousor philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions

and offences (hereinafter “sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 ***Onward transfers***

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant toArticle 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legalclaims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the datasubject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 ***Documentation and compliance***

(a) The data importer shall promptly and adequately deal with enquiries from the data exporterthat relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried outon behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered bythese Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certificationsheld by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 8

[MODULE THREE: Transfer Processor to Processor]

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 ***Instructions***

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter

8.2 *Purpose limitation*

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 *Transparency*

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 *Accuracy*

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 *Duration of processing and erasure or return of data*

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 *Security of processing*

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the

data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 ***Sensitive data***

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 ***Onward transfers***

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union(in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(a) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(b) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(c) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(d) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 ***Documentation and compliance***

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9
[MODULE TWO: Transfer Controller to Processor]

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub- processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub- processors at least 15 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for,in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub- processor agreement and any subsequent amendments to the data exporter. To the extentnecessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance ofthe sub-processor's obligations under its contract with the data importer. The data importershall notify the data exporter of any failure by the sub-processor to fulfil its obligations underthat contract.

(e) The data importer shall agree a third -party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processorcontract and to instruct the sub-processor to erase or return the personal data.

Clause 9
[MODULE THREE: Transfer Processor to Processor]

Use of sub-processors

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of subprocessors at least 15 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the subprocessor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

[MODULE TWO: Transfer Controller to Processor]

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received froma data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 10

[MODULE THREE: Transfer Processor to Processor]

Data subject rights

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance withthese Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the dataimporter shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or MemberState law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/hersubstantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/iesby any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled toreceive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and thedata subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subjectby breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from thedata importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liableand the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / theirresponsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits andcomply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmationthat the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clause

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country

of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain,the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; thestorage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available tothe competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to theseClauses and for the duration of the contract, it has reason to believe that it is or has becomesubject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request)indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend thedata transfer if it considers that no appropriate safeguards for such transfer can be ensured,or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferredpursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best effortsto obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The

data importer agrees to document its best efforts in orderto be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees toprovide the data exporter, at regular intervals for the duration of the contract, with as muchrelevant information as possible on the requests received (in particular, number of requests,type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority onrequest.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant toClause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to complywith these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination,applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under theapplicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the requestfor disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to thecompetent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible whenresponding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with theseClauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this rightto termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant toparagraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its

entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the EuropeanCommission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allowsfor third-party beneficiary rights. The Parties agree that this shall be the law of the Czech Republic.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the of the Czech Republic.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: The entity identified as "Customer" in the Agreement.

Address: The address for Customer associated with its account or as otherwise specified in the Agreement.

Contact person's name, position and contact details: The contact details associated with Customer's account, or as otherwise specified in the Agreement.

Activities relevant to the data transferred under these Clauses: The activities specified in Section 3 of the DPA.

Signature and date: By using Lens Spaces services, the data exporter will be deemed to have signed this Annex I.

Role (controller/processor): Controller or Processor

Data importer(s):

Name: "Mirantis" as identified in the DPA

Address: The address of Mirantis specified in the DPA

Contact person's name, position and contact details: Data Protection Officer, dataprivacy@mirantis.com.

Activities relevant to the data transferred under these Clauses: The activities specified in Section 3 of the DPA.

Signature and date: By making Lens Spaces available to the data exporter, the data importer will be deemed to have signed this Annex I.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Categories of data subjects are specified in Section 3 of the DPA.

Categories of personal data transferred

The personal data is described in Section 3 of the DPA.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The data exporter agrees in the DPA not to transfer any sensitive data.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Personal data is transferred in on continuous basis with frequency in accordance with Customer's instructions.

Nature of the processing

The nature of the processing is described in Section 3 of the DPA

Purpose(s) of the data transfer and further processing

The purpose of the data transfer is to provide the Services

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine

that period

As determined by the data exporter in accordance with the terms of the DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The subject matter, nature of processing and duration of the processing are described in Annex 2 of the DPA. Duration of the sub-processing is the whole period of processing by the data importer.

C. COMPETENT SUPERVISORY AUTHORITY

Where the data exporter entering into the Agreement is established in EEA, UK or Switzerland or the transfer falls within the territorial scope of application of such a country – the competent supervisory authority with responsibility for ensuring compliance by the data exporter with the Applicable Data Protection Laws as determined by the Applicable Data Protection Laws.

The parties agree that data exporter will not export to data importer, and data importer will not process on behalf of the data exporter, any personal data of data subject in relation to the offering of goods or services to them, or whose behavior is monitored and for this purpose, it is not relevant to determine an alternative competent supervisory authority under Sec. 13.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Security measures are described in Annex 1 to the DPA