STANDARD CONTRACTUAL CLAUSES

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 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 (General Data Protection Regulation) 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 integral part 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 add or 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 other clauses 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 - Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 13.1(c), (d) and (e);

(iv) Clause 14(e);

(v) Clause 16.

(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 terms shall 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 obligations provided 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

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

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 shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (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 of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 10

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.

Clause 11

Liability

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

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) 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 liable and the data subject is entitled to bring an action in court against any of these Parties.

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

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

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

Clause 12

Local laws and practices affecting compliance with the Clauses

(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; the storage 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 to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject 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 the data 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 14(d) and (e) shall apply.

Clause 13

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

13.1 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 transferred pursuant 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 efforts to 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 order to 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 to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant 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 on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 12(e) and Clause 14 to inform the data exporter promptly where it is unable to comply with these Clauses.

13.2 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 the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 12(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for 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 the competent supervisory authority on request.

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

SECTION IV – FINAL PROVISIONS

Clause 14

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, 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 12(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 right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. 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 European Commission 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 15

Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

Clause 16

Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of Germany.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name: LucaNet AG

Address: Karl-Liebknecht-Str. 14. , 10178 Berlin, Germany

Contact person's name, position and contact details: Legal & Compliance Department, legal@lucanet.com

Activities relevant to the data transferred under these Clauses: Performance of LucaNet.Consulting services for LNCS

Role (controller/processor): processor

Data importer(s):

1. Name: Customer (as specified in the customer agreement)

Address: as specified in the customer agreement

Contact person's name, position and contact details: as specified in the customer agreement

Activities relevant to the data transferred under these Clauses: Use of LucaNet.Cloud and LucaNet.Consulting consulting services

Role (controller/processor): controller

For the purposes of these Clauses, the Parties agree that the applicable module of the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914 is **Module Four (4) – Processor to Controller**. LucaNet AG acts as data exporter in its capacity as processor, and the Customer acts as data importer in its capacity as controller. The Parties acknowledge that the obligations set out in these Clauses shall be interpreted and applied accordingly.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Employees of the controller
- Employees of business partners of the controller
- Users of the products and services that are the subject of the commissioned processing
- other persons whose data are processed in the course of providing the agreed service

Categories of personal data transferred

- Name
- Contact details
- Contract data
- Invoice data
- Support requests
- Log data
- personal data contained in financial accounting systems
- other personal data made available by the controller to the processor in the course of providing the service agreed in the customer agreement

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.

not applicable

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

on a continuous basis to provide the service agreed in the customer agreement

Nature of the processing

- Storage/hosting (LucaNet.Cloud)
- Recording, organisation, structuring, retrieval, consultation, alignment or combination (LucaNet.Consulting)

Purpose(s) of the data transfer and further processing

Provision of the service agreed in the customer agreement. The purposes listed below only apply if they are relevant to the contractual relationship with the respective Customer.

- Provision of the financial performance management software for consolidated financial statement preparation, financial planning, analysis and reporting in the LucaNet.Cloud including provision of the LucaNet server layer (LucaNet.Financial OLAP Server and LucaNet.Financial Warehouse) as licensed, configured and used by the controller and its users; troubleshooting (prevention, detection and correction of technical problems); continuous product improvements including provision of updates; ensuring reliability, quality and security of the licensed product
- Performance of the agreed LucaNet.Consulting services including planning, technical advice, guidance/training, data collection and validation, data migration, implementation, troubleshooting and customer specific software development

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

The duration of the processing shall be governed by the customer agreement and the instructions of the controller.

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

not applicable

Supplement to the Standard Contractual Clauses (applicable to Singapore customers only)

1. Definitions

1.1 "**Authorised Users**" means the Customer, if it is a sole proprietor; or if otherwise, the Customer's employees, agents and independent contractors who are authorised by the Customer to use the Services.

1.2 "**General Purpose**" means purposes such as:

(a) carrying out due diligence or other screening activities (including background checks) in accordance with legal or regulatory obligations or risk management procedures that may be required by law and hence may have been put in place by (i) in the case of LucaNet by LucaNet; and/or (ii) in the case of the Customer by the Customer;

(b) dealing with, administering or carrying out an legally required internal or external audit of the Party's processes or businesses (this is applicable to LucaNet for LucaNet's internal or external audit; and applicable to the Customer for the Customer's internal or external audit);

(c) preventing or investigating any fraud, unlawful activity or omission or misconduct, including whether or not there is any suspicion of the aforementioned;

(d) complying with or as required by any applicable law, governmental or regulatory requirements of any relevant jurisdiction (whether Singapore or a non-Singapore country), including meeting the requirements to make disclosure under the requirements of any law (whether Singapore or non-Singapore) binding on the Party and/or for the purposes of any guidelines issued by regulatory or other authorities, whether in Singapore or elsewhere, with which the Party is expected to comply;

(e) complying with or as required by any request or direction of any governmental authority (whether Singapore or non-Singapore); or responding to requests for information from public agencies, ministries, statutory boards or other similar authorities, with which the Party is expected to comply. For the avoidance of doubt, this means that the Party may or will disclose the relevant personal data to the aforementioned parties upon their request or direction; and/or

(f) storing, hosting, backing up (whether for disaster recovery or otherwise) of the individual's personal data, whether within or outside Singapore.

1.3 "**PDPA**" means the Singapore Personal Data Protection Act 2012 including all subsidiary legislation related thereto.

1.4 "**Service Purpose**" means the purposes of: (i) dealing with, managing or administering the Services; and/or (ii) conducting analytics to improve the Services.

1.5 "**User Account**" means the account created by or for an Authorised User in order to access and use the Services, which is subject to these Terms and/or such other terms or guidelines which may be issued by LucaNet from time to time.

2. Personal Data Protection

2.1 If LucaNet processes any personal data on the Customer's behalf when performing the Services, the Parties record their intention that LucaNet shall be the Customer's data intermediary. The Customer agree to the following:

(a) that the personal data may be transferred or stored outside Singapore to LucaNet's affiliated entities, third party service providers or agents, for one or more of the Services Purposes or the General Purposes, or in order to carry out the Services;

(b) the Customer shall ensure that LucaNet may lawfully use, process and transfer the personal data in accordance with these Terms on the Customer's behalf; and

(c) the Customer shall ensure that the individuals whose personal data are being transferred overseas have been informed of, and have given their consent to, such use, processing, and transfer as required by all applicable data protection legislation including the PDPA.

2.2 The Customer represents and warrants that:

(a) for personal data of any Authorised Users and/or any other individuals that the Customer discloses to LucaNet or that the Customer discloses to LucaNet in the course of accessing and using the Customer's User Accounts (if applicable) and/or accessing and using the Services, that the Customer would have prior to disclosing such personal data to LucaNet obtained consent from the individuals whose personal data are being disclosed, to:

(i) permit the Customer to disclose the individuals' personal data to LucaNet for the Services Purposes and the General Purposes; and

(ii) permit LucaNet to collect, use, disclose and/or process the individuals' personal data for the Services Purposes and the General Purposes, including disclosing the said personal data to LucaNet's affiliated entities, third party service providers or agents, which may be sited outside of Singapore, for the Services Purposes and the General Purposes and such affiliated entities, third party service providers or agents of LucaNet processing their personal data for the Services Purposes and the General Purposes;

(b) any personal data of individuals that the Customer will be or are disclosing to LucaNet are accurate; and

(c) for any personal data of individuals that the Customer discloses to LucaNet, that the Customer is validly acting on behalf of such individuals and that the Customer has the authority of such individuals to provide their personal data to LucaNet and for LucaNet, its affiliated entities, third party services providers and agents to collect, use, disclose and process such personal data for the Services Purposes and the General Purposes.

2.3 For the avoidance of doubt, any reference to 'the Customer' in sub-paragraphs (a) to (c) under clause **[2.2]** is also a reference to the Authorised Users.

ANNEX II

Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of the Data

Description of the technical and organisational security measures implemented by the processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons. Examples of possible measures:

https://www.lucanet.com/fileadmin/user_upload/assets/legal_documents/it-security-guideline-lucanet.pdf

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller.

Description of the specific technical and organisational measures to be taken by the processor to be able to provide assistance to the controller.

https://www.lucanet.com/fileadmin/user_upload/assets/legal_documents/it-security-guideline-lucanet.pdf
https://d1.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf