Data Processing Terms and Conditions

Whereas Customer and Centric Software:

(i) have entered into an Agreement whereby Centric Software is providing software licenses, maintenance, hosting, and/or services to Customer,

(ii) wish to modify and/or supplement certain provisions of the Agreement and therefore amend it for the purpose of providing Customer with the necessary documentation related to the processing of Customer's Personal Data (as defined below) by Centric Software on behalf of Customer.

These Terms and Conditions (“DPA”) include the Standard Contractual Clauses as attached in Appendix 1.

Now, therefore, the parties hereto agree as follows:

1. Definitions

“Applicable Data Protection Legislation” means the General Data Protection Regulation (EU) 2016/679 (“GDPR”) and any delegated and implementing acts adopted in accordance with the GDPR and any other applicable data protection laws and all other regulations that may be applicable to the Processing implemented.

“Agreement” : The Master License and Services Agreement between Customer and Centric Software under the terms of which Centric Software provides software licenses, maintenance, hosting, and/or services to Customer.

“Commission”, “Controller”, “Data Subject”, “Personal Data”, “Process/Processing” “Processor”, “Supervisory Authority” and “Personal Data Breach” shall have the same meaning as in the Applicable Data Protection Legislation.

“Customer’s Personal Data” means any Personal Data provided by Customer (or any Customer’s authorized user) to Centric software through Customer’s use of Centric Software's software licenses, hosting, and/or services, as detailed in Appendix 2.

"EEA" means the European Economic Area, which consists in European Union, Liechtenstein, Iceland and Norway.

“Standard Contractual Clauses” means the Standard Contractual Clauses (module 2: Controller to Processor) pursuant to Commission implementing decision (EU) 2021/914 of 4 June 2021, as
attached in Appendix 1 (with its Annexes incorporated into Appendixes 2 and 3 of this DPA), which the parties agree may be replaced or updated in accordance with a relevant European Commission decision.

“Sub-Processor” means any Processor appointed by Centric Software or by any other Centric Software's Sub-Processor, which receives, from Centric Software or from any other Centric Software's Sub-Processor, Customer's Personal Data for the sole and exclusive purpose of performing Processing on behalf of Customer after the transfer in accordance with the terms of this Agreement and a written subcontract between such Sub-Processor and the Processor.

“Technical and Organizational Measures” (TOMs) means those appropriate measures that are aimed at Processing Customer’s Personal Data in compliance with the Applicable Data Protection Legislation, as detailed in Appendix 3.

“Transfer” means (i) a transmission of Customer’s Personal Data from Customer to Centric Software, or (ii) an onward transmission of Customer's Personal Data from Centric Software to a Sub-Processor, or between two Sub-Processors.

“Transfer Impact Assessment” means the transfer impact assessment required pursuant to Clause 14 of the Standard Contractual Clauses which may be updated from time to time by the parties with new or updated information.

The word "include" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

Defined terms can be used in a singular or plural form.

2. Scope

This DPA applies where and only to the extent that Centric Software processes Customer’s Personal Data on behalf of Customer in the course of providing software licenses, hosting, and/or services to Customer and such Customer's Personal Data is subject to the Applicable Data Protection Legislation. Accordingly, Customer is the Controller of Customer's Personal Data and Centric Software shall process Customer's Personal Data as Processor.

3. Centric Software’s Obligations

Centric Software, as Processor, will:

- to the maximum extent permitted by Applicable Data Protection Legislation and for the duration of the Processing of Customer's Personal Data, collect, store and Process Customer's Personal Data in accordance with the Agreement and this DPA, and Customer's written reasonable instructions, which shall in all circumstances be consistent with such Agreement;
- ensure that access to Customer’s Personal Data is limited to its employees, agents or contractors who need to know the relevant Customer’s Personal Data, as necessary for the purposes of the Agreement and who are bound by an appropriate obligation of confidentiality;
• reasonably assist Customer in complying with its obligations as Controller under sections 32 through 36 of the GDPR, taking into account the nature of Processing as described in the Agreement. If Centric has reason to believe or is convinced that a Personal Data Breach impacting Customer has occurred, Centric will (i) notify Customer of the incident without undue delay after becoming aware of such Personal Data Breach and (ii) provide Customer with available information allowing it to comply with its notification obligations with the competent supervisory authority;
• reasonably assist Customer to fulfil its obligations in responding to requests from Data Subjects to exercise their rights under Applicable Data Protection Legislation in a manner consistent with the use of the Centric Software's software licenses, hosting, and/or services and Centric Software's role as Processor;
• make available to Customer all necessary information in its possession to demonstrate Customer’s compliance with its obligations provided for by the Applicable Data Protection Legislation and reflected in this section and, in the event compliance with Applicable Data Protection Legislation cannot be shown through the appropriate documentation provided by Centric Software, allow for, an audit. Such audits will be subject to the following cumulative conditions:
  o Customer shall provide Centric with at least thirty (30) days prior written notice;
  o the scope of such audit shall be limited to assessing Customer’s compliance with the Applicable Data Protection Legislation in the specific subject area where the documentation provided by Centric was not sufficient;
  o such audit shall be conducted by an independent auditor that is not a Centric Software’s competitor named by Customer at Customer’s cost; and
  o such audits may not be performed more than once every twelve (12) months.

Appendix 2 to this DPA sets out certain information regarding Centric Software’s Processing of Customer’s Personal Data as required by the article 28(3) of the GDPR.

4. Customer’s Obligations

Customer acknowledges and agrees that it is and shall at all times remain the sole Controller of Customer’s Personal Data, that will be Processed as part of its access to and use of Centric Software's licenses, hosting and/or services and therefore, Customer shall be responsible for complying with all Applicable Data Protection Legislation including, but not limited to, (i) Transfer of Personal Data, (ii) information of Data Subjects and (iii) access, modification and deletion rights of Data Subjects. Centric Software as Processor will collect, store and Process the Personal Data in accordance with the Agreement and this DPA.

5. Data Subjects Rights

When Centric Software receives a request from a Data Subject for access to, correction, update or erasure of their Personal Data or a request to restrict Processing, Centric Software will, to the extent legally permitted, promptly notify Customer and redirect Data Subject’s request to Customer.

To the extent Customer does not have the ability to independently correct, amend, or delete Customer’s Personal Data, or block or restrict Processing of Customer’s Personal Data, then at
Customer's written direction and to the extent required by Applicable Data Protection Legislation, Centric Software, as Processor, shall assist Customer to fulfil its obligations in responding to requests from Data Subjects to exercise their rights under Applicable Data Protection Legislation in a manner consistent with the performance of the Agreement. To the extent legally permitted, Customer shall be responsible for any reasonable costs arising from Centric Software's or its Sub-Processors' provision of such assistance.

6. **Sub-Processing**

Centric Software is a worldwide multi-tiered organization, located in the Americas, Asia and Europe. In that globalized context, in order for Centric Software to provide the software licenses, hosting, and/or services, Customer appoints Centric Software as Processor and agrees that Customer's Personal Data may be Transferred to, stored, accessed and Processed in any country in which Centric Software or its subcontractors are located. Centric Software will ensure that the same data protection obligations as set forth in this DPA shall be imposed on the Sub-Processors by way of a contract and/or the standard contractual clauses from the European Commission in such a manner that the Processing will meet the requirements of the Applicable Data Protection Legislation.

The list of the Sub-Processors, that may be involved in the Processing of Customer's Personal Data due to the Processing activities implemented on behalf of Customer and authorized by Customer at the Effective Date of this DPA is attached in Appendix 4. Centric Software will inform Customer of any intended changes concerning the addition of new Sub-Processors or replacement of existing Sub-Processors, thereby giving Customer the opportunity to object to such changes. Customer will be notified at least fifteen (15) days in advance before Centric Software authorizes any new Sub-Processor to Process Customer's Personal Data, except in case of emergency. Customer may reasonably object to Centric Software's use of a new Sub-Processor if (i) such new Sub-Processor Processes Customer's Personal Data and (ii) Customer demonstrates it has a legitimate interest in objecting to this new Sub-Processor and notifies Centric in writing, within fifteen (15) days after receipt of the notification. In the absence of an objection from Customer, the new Sub-Processor shall be deemed to be accepted by Customer. If Customer notifies Centric Software of its objection to the new Sub-Processor within the above timeframe, Customer may terminate Centric Software's license, hosting, and/or services impacted by this change of Sub-Processor before the end of the notice period specified herein.

7. **Security**

Centric will implement and maintain appropriate TOMs, as attached in Appendix 3. Such TOMs are designed to protect Customer's Personal Data from a Personal Data Breach and to help ensure the ongoing confidentiality, integrity, and availability of the Customer's Personal Data and Processing systems.

Customer acknowledges that the Centric Software's TOMs are subject to technical progress and development and that Centric Software may update or modify them from time to time provided that such updates and modifications do not result in the degradation of the overall security of the measures implemented by Centric Software.

8. **Term and termination of this DPA**
This DPA comes into force on the Effective Date, as specified above, and will continue for the term of the Agreement.

Upon termination or expiration of the Agreement, Centric Software will:

- at Customer's option, either delete or return all Customer's Personal Data to Customer; and
- delete all existing copies, of Customer's Personal Data in its possession in accordance with the terms and timelines of such Agreement, except (i) where applicable law requires retention of Customer's Personal Data or where Customer's Personal Data is necessary for evidentiary purposes during the applicable statute of limitations, and (ii) except for automated system backup copies that may not with reasonable efforts be destroyed, provided, however, that such copies are not accessed or used by Centric Software and are destroyed in due course in accordance with Centric Software's standard document destruction policies and practices.

In any event, Centric Software will maintain Customer's Personal Data securely and protect it from any further Processing for as long as Centric Software retains such Personal Data. The terms of this DPA shall survive for so long as Centric Software continues to retain any of Customer's Personal Data.

9. Liability

Any claims arising out of, in connection with, or related to this DPA, whether in contract, tort or under any other theory of liability are subject to the terms and conditions, including but not limited to the exclusions and limitations, set forth in the Agreement.

In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise. Customer shall indemnify Centric Software, as applicable, against any and all such claims or costs of any kind that exceed the exclusions and limitations set forth in the Agreement.

Centric Software shall not be liable for the damage caused by a Processing and/or in case of non-compliance with the Applicable Data Protection Legislation as a result of a Processing resulting in an administrative fine issued by a Supervisory Authority or a court against Customer unless such damage or non-compliance directly results from:

- Acts of Centric Software beyond or contrary to Customer's written instructions;
- Failure of Centric Software's employees to comply with their applicable confidentiality obligations;
- Partial or total non-performance of the TOMs agreed to between the Parties as set out in the Agreement.

When Customer and Centric Software are liable (i) for the damage caused by the Processing to one or several Data Subjects and/or (ii) in case of non-compliance with the Applicable Data Protection Legislation as a result of a Processing resulting in an administrative fine finally awarded by a Supervisory Authority or a court against one party, the parties agree to negotiate in good faith the determination of the portion of liability corresponding to the share of responsibility of each party in the execution of the damage and/or the non-compliance and, if applicable, of the amount due by
one party to the other party for compensation, within six (6) months from notification by one party
to the other party. Upon the failure of the parties to agree on the determination of the quantum,
within the aforementioned time period, the parties may decide to submit the determination of the
quantum corresponding to the share of liability of each party to the court of competent jurisdiction
as determined in this DPA.

10. Miscellaneous

- Customer acknowledges and agrees that nothing in the Agreement or this DPA shall prevent
  Centric Software from exercising its right to use and disclose Personal Data relating to
  and/or obtained in connection with the operation, support and/or use of the Centric
  Offerings for its legitimate business purposes, including billing, account management,
  technical support, product development, sales and marketing.
- **Entire agreement.** Except for the changes made by this DPA, the Agreement remains
  unchanged and in full force and effect. If there is a discrepancy, inconsistency or
  contradiction between this DPA and the Agreement, the provisions of this DPA shall prevail,
  but solely with respect to the purpose of this DPA. In addition, it is explicitly agreed that in
  case of discrepancy, inconsistency or contradiction between the Standard Contractual
  Clauses and the DPA, the Standard Contractual Clauses shall prevail.
- **Severability.** If any provision of this DPA is found by a court of competent jurisdiction or
  arbitrator to be illegal, void or unenforceable, the other provisions shall remain in full force
  and effect, and the affected provision will be modified so as to render it enforceable and
  effective to the maximum extent possible in order to effect the original intent of the parties.
- **Governing law and jurisdiction.** This DPA shall be governed by and construed in
  accordance with governing law and jurisdiction provisions in the Agreement, unless required
  otherwise by the Applicable Data Protection Legislation.
APPENDIX 1 – STANDARD CONTRACTUAL CLAUSES

(Module 2: Controller to Processor)

Section I

Clause 1

Purpose and Scope

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.

The Parties:

1. 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 Appendix 2, Section A (hereinafter each “data exporter”), and
2. 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 Appendix 2, Section A. (hereinafter each “data importer”)

Clause 2

Effect and invariability of the Clauses

1. 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.
2. 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

1. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
2. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

**Clause 4**

Interpretation

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

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

3. 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 Appendix 2, section B.

**Clause 7**

Optional Docking clause

1. 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 Appendix 2, section A.

2. Once it has completed the Appendix and signed Appendix 2, section 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 Appendix 2, section A.

3. 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 organizational 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 the data exporter. The data exporter may give such instructions throughout the duration of the contract.

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 Appendix 2, section 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 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 the measures described in Appendix 3 and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the 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 Appendix 2, section 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 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 organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized 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 personal data 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 organizational measures specified in Appendix 3. 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 personal 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 authorized 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 the data exporter without undue delay 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 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 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 described in Appendix 2, Section 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:

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 Regulation of (EU) 2016/679 with respect to the processing in question;
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 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 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 by these 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 certifications held 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 9

Use of sub-processors

a) The data importer has the data exporter’s general authorization 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 (fifteen) 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 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 sub-processor 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

Data subject rights

a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorized 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 Appendix 3 the appropriate technical and organizational 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 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 authorized 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 with these 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 data importer shall accept the decision of the data subject to:

   a. 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;

   b. 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, organization 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 Member State law.

f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive 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/ies by any breach of these Clauses.

b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive 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 the data 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 subject by 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 the data 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 liable and 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 / their responsibility 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 Appendix 2, section 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 Appendix 2 section 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 behavior is monitored, are located, as indicated in Appendix 2, section 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 and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that 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 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 authorizing 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:

c) 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;

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

e) any relevant contractual, technical or organizational 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.

f) 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.

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

h) 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).

i) 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 organizational 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 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 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 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.
15.2 Review of legality and data minimization

(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 14(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 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 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 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:

- the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph
- and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
- the data importer is in substantial or persistent breach of these Clauses; or
- 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 that has been transferred prior to the termination of the contract pursuant to paragraph (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 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 17
Governing Law

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

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. The Parties agree that those shall be the courts of X.

(b) 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.

(c) The Parties agree to submit themselves to the jurisdiction of such courts.
APPENDIX 2 – INFORMATION ABOUT PROCESSING OF CUSTOMER’S PERSONAL DATA
(at the same time Annex I to the Standard Contractual Clauses)

LIST OF PARTIES

Data exporter(s):
Name: [Customer, as defined in the Agreement]
Address: [Customer address as defined in the Agreement]
Contact person’s name, position and contact details: [TO BE COMPLETED]
Activities relevant to the data transferred under these Clauses: Data is transferred to allow data importer to provide the software products and/or services under the Agreement.

Data importer(s):
Name: Centric Software, as defined in the Agreement
Address: Centric Software, as defined in the Agreement
Contact person’s name and position: Ron Watson, DPO
Centric Software’s Data Protection Officer may be contacted:
  • by mail: privacy@centricsoftware.com
Activities relevant to the data transferred under these Clauses: Processing of Customer Personal Data, solely pursuant to the Agreement.

DESCRIPTION OF TRANSFER

Categories of Data Subjects whose Personal Data is Processed
Data Subjects may include:
  • Customer's authorized users, including employees, contractors, collaborators, partners, stakeholders and/or customers of the Customer, depending on the terms of the Agreement and on Customer's use of Centric Software's software licenses, hosting, and/or services;
  • Any other Data Subject whose Personal Data is included in Customer Personal Data.

Categories of Personal Data Processed
The categories of Personal Data that may be Processed by Centric as Processor, depending on Customer's use of the software products and/or services, are the following:
  • First name, last name;
• Email address;
• Job title;
• Phone number;
• Connection data (IP address, logs, etc.);
• Online identifies (user ID);
• Password;
• Address

Depending on the terms applicable to each release of Centric Software's software licenses, hosting, and/or services, Customer may elect to provide Centric Software with other categories of Personal Data.

However, Customer acknowledges and agrees that the Centric Software's Offerings are not dedicated to Process any sensitive Personal Data or special category of data, as defined by the Applicable Data Protection Legislation, unless a dedicated written agreement is executed between the parties.

**Nature and Purpose of the Processing**

Making software licenses available, whether on-premise or on a hosted basis, providing technical support for Centric Software's software products and providing consulting services for implementation of such software. Hosting Customer data where hosting is purchased.

Centric Software Processes Personal Data to provide the software products and/or services as specified under the Agreement.

Depending of the software products and/or services ordered by Customer, Centric Software will Process Customer Personal Data for the following purposes:

• Collection, access, use, storage and deletion of Customer Personal Data;
• Authentication mechanism.

**Duration of the Processing**

Centric Software Processes Personal Data for the duration of the software licenses, hosting, and/or services as specified under the Agreement. Upon termination or expiration of the Agreement, Centric will delete all Customer's Personal Data to Customer in accordance with the terms and timelines of such Agreement, except where applicable law requires retention of such Customer's Personal Data or where such Customer's Personal Data is necessary for proof purposes during the applicable statute of limitation.

Customer may retrieve Customer's Personal Data pursuant to the procedures described in the documentation of Centric Software's software licenses, hosting, and/or services and, as the case may be.

**For Processing by Sub-Processors, also specify subject matter, nature and duration of the Processing**
In order to provide the software products and/or services, Centric Software may appoint other companies as Sub-Processors which may receive, from Centric Software or from any other Sub-Processor of Centric Software, Personal Data for the sole and exclusive purpose to Process activities to be carried out on behalf of Customer in accordance with the terms of the Agreement and the terms of a written subcontract.

Centric Software will ensure that the same data protection obligations as set forth in the Agreement shall be imposed on the Sub-Processors by way of a contract and/or the standard contractual clauses from the European Commission in such a manner that the Processing will meet the requirements of the Applicable Data Protection Legislation.

The list of Sub-Processors is available in Appendix 4 of this DPE.

**Competent Supervisory Authority**

Supervisory authority with responsibility for ensuring compliance by the data exporter, as provided in Clause 13 of the Standard ContractualClauses.
APPENDIX 3 - TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA
(at the same time Annex II to the Standard Contractual Clauses)

The description of the technical and organizational measures Centric Software has implemented are listed below.

Customer is entitled to subscribe to changes to obtain notice of updates implemented by Centric to those measures.

The technical and organizational measures may also be completed by specific terms as detailed in the documentation associated to each release of the software products and/or services ordered by Customer.

1. **Confidentiality (Article 32(1) lit. (b) GDPR)**
   - Physical Access Control

   No unauthorised access to Data Processing Facilities
   - Issue of physical keys to authorized personnel with a need to access applicable facility(ies);
   - Door locking of facilities to prevent unauthorized access;
   - All visitors are collected at reception, accompanied while on-site, and limited to areas necessary for the purpose of their visit
   - Office doors and windows closed when workers are not in the facility.
   - Electronic Access Control to systems

No unauthorised use of the Data Processing and Data Storage Systems
   - Authorization concept where access to systems is provided on a need to know basis;
   - Defined process for allocation of user accounts;
   - Computers and mobile devices secured by password;
   - Securing of network connections (e.g. remote access).
   - Internal Access Control (permissions for user rights of access to and amendment of Personal Data)

No unauthorised Reading, Copying, Changes or Deletions of Personal Data within the system
   - Differentiated access rights (profiles, roles, transactions and objects)
   - Rights authorisation concept based on need to know.
   - Isolation Control
The isolated Processing of Data, which is collected for differing purposes

- Data segregated by function (maintenance support / consulting services / hosting services)
- Keeping customer data separate (though may be stored on the same systems) to enable customer to exercise rights regarding deletion.

2. **Integrity (Article 32(1) lit. (b) GDPR)**
   - Data Transfer Control
   No unauthorised Reading, Copying, Changes or Deletions of Personal Data with electronic transfer or transport
   - Encryption/tunneling (Virtual Private Networks (VPN))
   - Utilization of secure FTP
   - Data Entry Control
   - Differentiated access rights (profiles, roles, transactions and objects) by Agent personnel

3. **Availability and Resilience (Article 32(1) lit. (b) GDPR)**
   - Availability Control
   Prevention of accidental or willful destruction or loss
   - Email backups
   - Backups of data logged into the support services portal
   - Where Managed Hosting Services are being provided, options for backup strategy and disaster recovery are available to customer for data they input into the Licensed Software
   - Worker computers have anti-virus software
   - Firewall systems
   - Rapid Recovery (Article 32(1) lit.(c) GDPR) (disaster recovery plan)
     - Disaster recovery plan for all key Agent business systems
     - Disaster recovery options available for Principal where Managed Hosting Services have been ordered and paid for.

4. **Procedures for regular testing, assessment and evaluation (Article 32(1) lit. (d) GDPR; Article 25(1) GDPR)**
• Annual penetration and security vulnerability testing of Centric8 PLM software
• System monitoring of critical Agent systems
• System monitoring of Principal systems being hosted through Agent’s Managed Hosting Services
• Incident Response Management
• Order or Service Agreement Control

No third party data processing as per Article 28 GDPR without corresponding instructions from the Client

• Controls on the selection of the Service Provider, duty of pre-evaluation;
• Availability of resources to discuss with Principal third party data processing scope;
• Principal may request access to evaluate third party data processing protections.

5. Data Protection by Design and Default (Article 25 (1) and (2) GDPR)

Agent reasonably limits use of personal data and internal access to Principal personal data to that necessary for each specific purpose of processing.

The Centric8 PLM software has enabled data encryption during transmission.

The Centric8 PLM software can also encrypt data stored within it at rest upon Principal’s election. Principal must make this election in writing.
APPENDIX 4 - LIST OF AUTHORISED SUB-PROCESSORS
(at the same time Annex III to the Standard Contractual Clauses)

The list of the Sub-Processors that may be involved in the Processing of Customer’s Personal Data due to the Processing activities implemented by Centric Software on behalf of Customer are listed below.

Customer is entitled to subscribe to changes to obtain notice of any intended changes concerning the addition or replacement of other Sub-Processors.
<table>
<thead>
<tr>
<th>Name</th>
<th>Address</th>
<th>Nature and Type of Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Web Services, Inc.</td>
<td>410 Terry Avenue North Seattle, WA 98109-5210 USA</td>
<td>Hosting Services</td>
</tr>
<tr>
<td>Google LLC, Google Ireland Limited, Google Asia Pacific Pte. Ltd.,</td>
<td>GORDON HOUSE, BARROW STREET, DUBLIN 4, DUBLIN, D04E5W5, IRELAND</td>
<td>Hosting Services</td>
</tr>
<tr>
<td>Microsoft Corporation</td>
<td>ONE MICROSOFT WAY REDMOND WA 98052</td>
<td>Hosting Services &amp; Email Provider</td>
</tr>
<tr>
<td>Digital BH 800, LLC (Digital Realty)</td>
<td>2805 Lafayette St Santa Clara CA 95050 USA</td>
<td>Hosting Services</td>
</tr>
<tr>
<td>Rackspace US, Inc.</td>
<td>1 Fanatical Place City of Windcrest San Antonio, TX 78218</td>
<td>Hosting Services</td>
</tr>
<tr>
<td>Kripya Engineering Private Ltd.</td>
<td>62, KGN Towers 3rd Floor B-Wing, Ethiraj Salai, Egmore, Chennai-600008 INDIA</td>
<td>Off-shore Technical Support</td>
</tr>
<tr>
<td>Atlassian Pty Ltd &amp; Atlassian, Inc</td>
<td>Level 6 341 George Street Sydney, NSW 2000 Australia 350 Bush St. Floor 13 San Francisco, CA 94104 United States</td>
<td>Jira &amp; Confluence applications (Technical Support &amp; Consulting Services)</td>
</tr>
<tr>
<td>Centric Software, Inc.</td>
<td>655 Campbell Technology Parkway, Suite 200 Campbell, CA 95008 USA</td>
<td>Technical Support, R&amp;D, Marketing activities, E-mail</td>
</tr>
<tr>
<td>Other Centric Software, Inc. entities may also act as Sub-Processors</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Centric Software Sub-Processor List**