

**PARTNER AND SUPPLIER Data Processing ADDENDUM**

This Data Processing Agreement including all Appendices, (hereinafter “**DPA**”) is entered into on <DPA Effective Date> **(“Effective Date**”) by and between <Contracting Party Name>, with its principal place of business located at <Contracting Party Address>, (hereinafter the “**Company**”) and <Centric Software Entity Name>, with its principal place of business located at <Centric Software Entity Address> (hereinafter “**Centric Software**”).

Company and Centric Software being also referred to as a “Party” individually and the “Parties” collectively.

Whereas Centric Software and Company:

1. have entered into an agreement [REFERENCE TO BE ADDED] (the “**Agreement**”) whereby Centric Software is contracting products and/or services to Company (hereinafter the “**Services**”),
2. wish to modify and/or supplement certain provisions of the Agreement and therefore amend it with this DPA for the purpose of providing Centric Software with the necessary documentation related to adequate safeguards in the course of the processing of Centric Personal Data (as defined below) including, if and when applicable, for the Transfer by Company of Centric Personal Data in third countries which do not ensure an adequate level of data protection.

Now, therefore, in order to provide adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the Processing, including Transfer, of Centric Personal Data in compliance with the Applicable Data Protection Legislation, the parties hereto have agreed as follows:

1. **DEFINITIONS**

"**Applicable Data Protection Legislation**" means any data protection laws and all other regulations that may be applicable to the Processing implemented, including, as applicable, the EU Data Protection Legislation.

"**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**","**Processing**", “**Processor**» and "**Supervisory Authority**" shall have the same meaning as in the Applicable Data Protection Legislation. If the preceding terms are not defined in the Applicable Data Protection Legislation, then such terms as used in this Agreement shall have the same meaning as their analogous terms under the Applicable Data Protection Legislation. In the event there are no such analogous terms then the definitions of those terms under GDPR shall apply.

### "**Centric Personal Data**" means any Personal Data and including Personal Data Processed by the Parties, pursuant to or in connection with the Agreement as detailed in **Appendix 1 “Details about the processing of Centric Personal Data”**.

### “**Country or Regional Specific Terms**” means the supplemental country or regional terms that may be applicable, as detailed in **Appendix 3 “International Transfer Mechanism”**.

### **“Company Affiliate”** means any business entity in which the Company, directly or indirectly, (i) owns more than 50% of the outstanding equity or ownership interest, or (ii) has the power to designate the managing authority. All Company Affiliates are listed in **Appendix 0 “List of Affiliates”**.

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

**“EU Data Protection Legislation”** means (i) the General Data Protection Regulation (EU) 2016/679 (“**GDPR**”) and any delegated and implementing acts adopted in accordance with the GDPR, (ii) the Swiss Federal Data Protection Act of 19 June 1992 and its Ordinance (“**Swiss FDPA**”); and (iii) in respect to the UK, the GDPR as saved into the United Kingdom law by virtue of section 3 of the United Kingdom’s European Union (Withdrawal) Act 2018 (“**UK GDPR**”) and the UK Data Protection Act 2018 (together the “**UK Data Protection Legislation**”); in each case as such laws may be amended or superseded from time to time.

"**Onward Company**"means any Onward Company of Company (including any third party and any Company Affiliate) appointed by Company (or by any other Onward Company of Company), which receives from Company, Centric Personal Data for the purpose of performing Processing on behalf of a Controller, in connection with the terms of the Agreement and the terms of a written contract between such Onward Company and the Company.

**“Public Authority”** means a government agency or law enforcement authority, including judicial authority.

**“Restricted Transfer”** means; (i) where the GDPR applies, a Transfer of Centric Personal Data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK Data Protection Legislation applies, a Transfer of Centric Personal Data from the UK to any other country which is not based on adequacy regulations pursuant to Section 17A of the UK Data Protection Act 2018; and (iii) where the Swiss FDPA applies, a Transfer of Centric Personal Data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.

**“Standard Contractual Clauses” or “SCCs”** means the Standard Contractual Clauses pursuant to Commission implementing decision (EU) 2021/914 of 4 June 2021available here: <https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en> as completed as set forth in Appendix 3 “International Transfer Mechanism”..

### **“Technical and Organizational Measures”** or “**TOMs**” means those appropriate measures that aimed at processing Centric Personal Data in compliance with the Applicable Data Protection Legislation including minimizing the Processing of Centric Personal Data and protecting them against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of Processing, including measures applied during transmission and to the Processing of Centric Personal Data in the country of destination. TOMs are as detailed in **Appendix 4** **”Technical and organizational measures to ensure the security of the Centric Personal Data**.

### "**Transfer**"means (i) a transmission of Centric Personal Data between the Parties, or (ii) an onward transmission of Centric Personal Data from a Party to another third party Controller, Processor or Sub-Processor. For cross-border Transfers, the Parties may also be designated in this Agreement as “**Data Importer**” and/or “**Data Exporter**” when a Data Exporter transfers Centric Personal Data to a Data Importer located in another country or region.

### **“Transfer Impact Assessment”** means the transfer impact assessment required pursuant to Clause 14 of the Standard Contractual Clauses as attached in **Appendix 6 “Transfer Impact Assessment”**, which may be updated from time to time by the parties with new or updated information.

**“UK Addendum”** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B1.0), in force 21 March 2022 issued by the Information Commissioner’s Office under S.119(A) of the UK Data Protection Act 2018, as updated or amended from time to time.

## 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.

Any other capitalized terms used in this DPA shall have the meaning defined in the Agreement.

1. **OBLIGATIONS OF THE PARTIES**

Each Party shall be responsible, for its Processing activities as Controller, for complying with all Applicable Data Protection Legislation.

When Centric Software is considered the sole Controller of the Centric Personal Data then Centric Software shall be solely responsible for determining the purpose and means of the processing.

When Centric Software and Company are considered Joint Controllers, from the start of the Agreement, of the Centric Personal Data then the Parties will jointly determine the purposes and the means of the processing as described in **Appendix 1 “Details about the processing of Centric Personal Data”**. In the event that Centric Software and Company become Joint Controllers due to unexpected events (for example, but not limited to, due to a court decision) then this DPA will automatically become a joint controller agreement (changing the relevant SCC if necessary) and to the extent possible Centric Software will continue to determine the purpose and the means of the processing.

Additionally, when required by Applicable Data Protection Legislation, each Party shall:

* ensure that Centric Personal Data is accurate, complete, strictly necessary for the specific, legitimate and lawful conduct of the Process and, where required, kept up to date;
* treat Centric Personal Data as confidential and restrict its disclosure to those of its employees, agents or other contractors who need to Process it and that have committed themselves to appropriate obligations of confidentiality;
* store Centric Personal Data in a structured, commonly used, and machine-readable format;
* observe the principle of data minimization within the meaning of Applicable Data Protection Legislation;
* keep a record of all categories of Processing activities carried out pursuant to this Agreement;
* take appropriate and reasonable technical and organizational measures, as described in this Agreement, to ensure the security of Centric Personal Data.

Each Party has designated the following contact person:

* For Company, the Data Protection Officer or equivalent may be contacted:

[please complete]

* For Centric Software, the Centric Software Data Protection Officer may be contacted:
  + by email: [privacy@centricsoftware.com](mailto:privacy@centricsoftware.com),
  + by mail: Centric Software Inc. – Privacy Team – 655 Campbell Technology Pkwy, Suite 200 Campbell CA 95008, USA.

1. **PROCESSING OF CENTRIC PERSONAL DATA**

This DPA defines the conditions under which Company commits to Process Centric Personal Data.

Company will:

* Process Centric Personal Data including its Transfer to Onward Companies according to the instructions and the requirements of this DPA, and
* Instruct each authorized Onward Company to comply with the requirements of this DPA, where applicable,

as strictly reasonably necessary for the provision of the products and/or services and consistent with the Agreement.

**Appendix 1 “Details about the processing of Centric Personal Data”** to this DPA sets out certain information regarding Centric Software’s Processing of the Centric Personal Data.

1. **COMPANY’S OBLIGATIONS**

According to the Applicable Data Protection Legislation and in addition to the Company’s obligations as detailed in the SCCs to the extent they are applicable, Company shall, at all time:

* Comply with the Applicable Data Protection Legislation in the Processing of Centric Personal Data including the “Privacy by Design principle” as mentioned in the Article 25 of the GDPR;
* Actively assist Centric Software in order to ensure Centric Software’s compliance with its obligations under the Applicable Data Protection Legislation;
* Process Centric Personal Data in accordance with Centric Software’s instructions;
* Ensure the reliability of all its employees, agents or contractors that may have access to Centric Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know and access the relevant Centric Personal Data, as necessary for the purposes of the Agreement and that those individuals have committed themselves to appropriate obligations of confidentiality no less stringent than those of the Agreement;
* Keep a record of all categories of Processing activities carried out pursuant to the Agreement.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Company shall implement TOMs to ensure a level of security appropriate to that risk, when relevant, the measures to protect Centric Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized use, disclosure or access, in particular, where the Processing involves the transmission of the data over a network, and against other unlawful forms of Processing as well as allow Centric Software to comply with its obligations as further detailed in this DPA. A description of TOMs is detailed in **Appendix 4**  **”Technical and organizational measures to ensure the security of the Centric Personal Data**.

1. **ONWARD COMPANY**

Company shall not Transfer to an Onward Company any Processing activity performed under this DPA without Centric Software’s prior specific written authorization. Company shall submit a request for specific authorization at least thirty (30) business days prior to any intended changes concerning the addition or replacement of any Onward Company, together with the information necessary to enable Centric Software to decide on the authorization.

The list of Onward Companies authorized by Centric Software at the Effective Date of this DPA is attached in **Appendix 5 “List of Permitted Onward Companies”**.

Company shall ensure at all times that each Onward Company carries out Processing activities on Centric Personal Data on behalf of Centric Software in compliance this DPA.

In the event of bankruptcy of Company or any similar event that affects the existence of Company, Company acknowledges and agrees that Centric Software shall still have the possibility to instruct Onward Company, including but not limited to deletion or return Centric Personal Data.

Company shall remain fully liable to Centric Software as regards the fulfillment of the obligations of the Onward Company and for the acts, errors and omissions of any Onward Companies to Process Centric Personal Data.

1. **DATA SUBJECT RIGHTS**

Taking into account the nature of the Processing, Company shall assist Centric Software for the fulfilment of Centric Software’s obligations to respond to Data Subject’s requests to exercise their rights under the Applicable Data Protection Legislation and, as applicable, the agreement between Centric Software and the Controller.

Company shall:

* Promptly notify Centric Software if it or one of its Onward Companies receives a request from a Data Subject in respect of Centric Personal Data;
* Ensure that it or any Onward Company does not respond to that request except on the documented instructions of Centric Software, or as the case may be Controller, or as required by Applicable Data Protection Legislation to which Centric Software or Company is subject to, in which case Company shall to the extent permitted by Applicable Data Protection Legislation inform Centric Software of that legal requirement before Company responds to the request; and
* Provide with the necessary information for Centric Software to address the request, as applicable.

1. **PERSONAL DATA BREACH**

Company shall notify Centric Software without undue delay - but in any case, no later than forty-eight (48) hours - upon becoming aware of an actual or suspected Personal Data Breach affecting Centric Personal Data and shall provide Centric Software with all necessary information to allow Centric Software to meet its legal obligations and/or any obligations to notify the Controller of the Personal Data Breach under the Applicable Data Protection Legislation.

Such notification shall as a minimum:

* Describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;
* Communicate the name and contact details of Company and/or Onward Company’s data protection officer or other relevant contact from whom more information may be obtained;
* Describe the likely consequences of the Personal Data Breach; and
* Describe the measures taken or proposed to be taken to address the Personal Data Breach, including where appropriate, measures to mitigate its possible adverse effects.

Company, and as applicable Onward Companies, shall co-operate with Centric Software and, as applicable, Controller and take such steps and measures as are directed by Centric Software and/or, as applicable, Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

In addition to the notification to Centric Software’s point(s) of contact Company is working with on a regular basis, an email shall be sent by Company to Centric Software’s Data Protection Officer at [privacy@centricsoftware.com](mailto:privacy@centricsoftware.com).

1. **AUDIT RIGHTS**

Company shall fully cooperate at all times and make available to Centric Software or its representatives with all the documents relating to the security of the Processed Centric Personal Data including, in particular, the necessary technical documentation, any updated information related to the Transfer Impact Assessment, the risk analysis produced and a detailed list of the security measures implemented.

Company shall make available to Centric Software upon request and at least once a year, all information necessary to demonstrate compliance with this DPA (including audits of its Onward Companies) and the Applicable Data Protection Legislation (including article 28(3)(h) of the GDPR), including but not limited to the updated GDPR and the security questionnaires as the case may be, and shall allow for and contribute to audits, including inspections, by Centric Software or an auditor mandated or authorized by Centric Software in relation to the Processing of the Centric Personal Data.

If Company is officially certified according to an international standard by a third party (such as ISO 27701 or any comparable or higher certification) applicable to the scope of the Agreement, it shall maintain current such status for the duration of the Agreement and made it available to Centric Software on an annual basis. In case of loss of certification, it shall immediately inform Centric Software.

Centric Software shall be entitled to conduct direct audits at Onward Companies and to issue instructions to Onward Companies directly.

1. **OBLIGATIONS IN CASE OF REQUESTS FOR ACCESS BY PUBLIC AUTHORITIES**

In the event the Company receives a request from a Public Authority for the disclosure of Centric Personal Data, the Company shall comply with the following process.

The Company agrees to promptly notify Centric Software if it:

## receives a request from a Public Authority, including judicial authorities, under the laws and regulations applicable to Company for the disclosure of Centric Personal Data; such notification shall include information about the Centric Personal Data requested, the requesting authority, the legal basis for the request and the response provided; or

## becomes aware of any access by Public Authorities to Centric Personal Data in accordance with the laws and regulations applicable to Company; such notification shall include all relevant information regarding such access which is available to Company.

## If Company is prohibited from notifying Centric Software under the laws and regulations applicable to the Company, the Company 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. Company agrees to document its best efforts in order to be able to demonstrate them on Centric Software’s request.

## Where permissible under the laws and regulations applicable to the Company, the Company agrees to provide Centric Software, at regular intervals for the duration of the Agreement, with as much relevant information as possible on the requests received (in particular, the number of requests, the type of data requested, the requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

## The Company agrees to preserve the information pursuant to this Section for the duration of the Agreement and make it available to the competent Supervisory Authority upon request unless legally prohibited to do so.

## The Company 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 and regulations applicable to the Company, applicable obligations under international law and principles of international comity. Company shall, under the same conditions, pursue possibilities of appeal. When challenging a request, Company 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 Centric Personal Data requested until required to do so under the applicable procedural laws and regulations.

## Company agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws and regulations applicable to the Company, make the documentation available to Centric Software. It shall also make it available to the competent Supervisory Authority on request unless legally prohibited from doing so.

## Company agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

To the extent legally permitted, Company shall inform Centric Software of an access request from a Public Authority to Centric Personal Data in a manner whereby Centric Software can, to the extent not prohibited by applicable laws, take adequate measures before a disclosure is made.

If Company receives a disclosure request from a Public Authority, Company shall enable Centric Software to conduct, if and when applicable, audits or inspections of its facilities and/or systems, on-site and/or remotely, to verify if Centric Personal Data was disclosed to Public Authorities and under which conditions.

To the extent possible and permissible by applicable law, Company shall assist the Data Subjects in their right to redress and examine their compensation requests as the case may be.

For the avoidance of doubt, this Agreement shall not require Company to pursue action or inaction that could result in civil or criminal penalty for Company such as contempt of court.

1. **INTERNATIONAL PROVISIONS**
   1. Jurisdiction Specific Terms**.** To the extent Company process Centric Personal Data originating from and protected by any Application Data Protection Legislation in one of the jurisdictions listed in **Appendix 2 “Jurisdiction Specific Terms”** of this DPA, the terms specified in **Appendix 2 “Jurisdiction Specific Terms”** with respect to the applicable jurisdiction(s) apply in addition to the terms of this DPA.
   2. Restricted Transfers. Either Party may make Restricted Transfers if it complies with the provisions on Restricted Transfers in applicable EU Data Protection Legislation and this DPA.  To the extent the Services require an onward transfer mechanism to lawfully transfer Centric Personal Data from an European jurisdiction (i.e., the European Economic Area*,*the United Kingdom, Switzerland) to a location outside of that jurisdiction (“**Transfer Mechanism**”), the terms set forth in **Appendix 3 “International Transfer Mechanisms”** of this DPA will apply.

The Parties have conducted a Transfer Impact Assessment to determine whether the Data Subjects, whose Personal Data is transferred, are afforded data protection rights that are essentially equivalent to the protection guaranteed within the European Union, taking into account the safeguards in place and the enforceable rights and effective legal remedies available to the relevant Data Subjects.

* 1. Additional technical and organizational measures. To the extent applicable to the Services, Company certifies that it has not purposefully created back doors or similar programming that could be used to access Centric Personal Data, or created or changed its business processes in a manner that facilitates access to Centric Personal Data. Company shall implement measures designed to ensure that they do not carry out any act or omission, which has or could reasonably be expected to have a material adverse impact on the security of Centric Personal Data. Company shall only store and access Centric Personal Data in accordance with required access policies and procedures as described in the TOMs, and with the use of required tools, as applicable.

Company shall have written contracts in place with its Onward Companies, which impose appropriate obligations in respect of Centric Personal Data, and which include the required transfer mechanisms under Applicable Data Protection Legislation for international data transfers.

1. **LIABILITY**

Any claims arising out of, in connection with, or related to this DPA, whether on contract, tort or under any theory of liability is subject to the terms and conditions, set forth in this DPA.

In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise. Company 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.

Each Party shall be liable to the other Party for any direct damages it causes by its material breach of this Agreement that are actually incurred by the other Party.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL EITHER PARTY HAVE ANY LIABILITY TO THE OTHER FOR INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES.

1. **TERMINATION OF THIS DPA**

Each Party shall promptly inform the other Party if it is unable to comply with this DPA, for whatever reason.

In the event that the Company is in breach of this DPA or unable to comply with this DPA (including, as applicable, the SCCs), Centric Software may suspend the Transfer of Centric Personal Data to the Company until compliance is ensured again.

Centric Software shall be entitled to terminate immediately this DPA in whole or part, in the following situations:

* it has suspended the Transfer of Centric Personal Data pursuant to this Section and compliance with this DPA (including, as applicable, the SCCs) is not reestablished within a reasonable time, but not later than one month after the suspension,
* the Company is in substantial or persistent breach of this DPA, or,
* the Company fails to comply with a binding decision of a competent court or the competent Supervisory Authority regarding its obligations under this DPA.

Company shall not be entitled to any compensation or damages as a result of such termination. Such termination shall be without prejudice to any damages or other remedies Centric Software may be entitled to.

In such case, Centric Personal Data that has already been transferred prior to the termination of this DPA shall be (at Centric Software's option) immediately returned to Centric Software or destroyed in its entirety. The same shall apply to any copies of the data.

The terms of this DPA shall survive for so long as the Company continues to retain the Centric Personal Data.

1. **EFFECTIVE DATE AND HIERARCHY**

This DPA comes into force on the Effective Date, as above specified, and will continue for the duration of the Processing of Centric Personal Data by Company pursuant to the terms of the 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.

1. **MISCELLANEOUS**

14.1. Should any provision of this DPA be invalid or unenforceable, then the other clauses of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties’ intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

14.2. This DPA cannot be assigned, for any reasons, without the prior written consent of the other Party. Any attempt to do so without such consent is null and void.

14.3. This Agreement and its amendments may be executed by electronic signature. Such executed agreements provided electronically shall be deemed an original.

**IN WITNESS WHEREOF**, the parties have caused this DPAto be executed by their duly authorized officers or representatives.

|  |  |
| --- | --- |
| **<Contracting Party Name>** | **<Centric Entity Name>** |
| Name of signatory: | Name of signatory: |
| Title: | Title: |
| Date: | Date: |
| Signature: | Signature: |

**APPENDIX 0 - LIST OF AFFILIATES**

* **LIST OF COMPANY AFFILIATES:**

|  |  |
| --- | --- |
| **Company Affiliate Name** | **Contact details** |
| <Company Affiliate Name> | <Company Affiliate Contact Details> |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**APPENDIX 1 - DETAILS ABOUT PROCESSING OF CENTRIC PERSONAL DATA**

1. **Subject matter, nature, purpose and duration of processing**

*Please provide a detailed description of the service the Company provides*

The Centric Personal Data shall be transferred and be retained for as long as necessary to fulfil the Agreement.

1. **Categories of Data Subject (indicate which are applicable)**

The group of individuals ("data subjects") affected by the processing of personal data under this Agreement includes:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ▢  ▢  ▢  ▢  ▢ | B2C/C2C Customers  User/Visitors of a B2C/C2C Website  Users/Visitors of a B2C/C2C App  B2C/C2C Prospects  Consultants/Advisors | ▢  ▢  ▢ | Employees (including temporary workers)  employees of contractors  (Job) Applicants | ▢  ▢  ▢  ▢  ▢ | B2B Customer  User/Visitors of a B2B Website  Users/Visitors of a B2B App  B2B Prospects  Suppliers/Subcontractors |
| ▢ | Others, namely: | | | | |

1. **Types of Customer Personal Data**

The following types Centric Personal Data shall be collected, processed and/or used under this Agreement:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ▢  ▢  ▢  ▢  ▢  ▢  ▢  ▢  ▢  ▢ | Name  Address information  (electronic) Contact information  Age/Date of Birth  Nationality  Order history  Account data  IP address  Profiles  Preference Data | ▢  ▢  ▢  ▢  ▢  ▢  ▢  ▢  ▢  ▢ | Billing/Payment data  Credit Card Information  Credit Risk Scoring  Voucher Data  Fraud data  Social Security Number  Criminal History Data  Health Data  Working Time  Resume Data | ▢  ▢ | Behavioural Data  [Art.9 GDPR](https://gdpr-info.eu/art-9-gdpr/) related data:  ▢ health data  ▢ racial or ethnic origin  ▢ political opinions  ▢ religious or philosophical beliefs  ▢ sexual orientation/ sex life  ▢ genetic/ biometric uniquely identifying data  ▢ trade union membership |
| ▢ | Others, namely: | | | | |

1. **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:**

Specific measures for sensitive data if stated under 3:

|  |  |
| --- | --- |
| ▢ strict purpose limitation  ▢ keeping a record of access to the data | ▢ access restrictions (including access only for staff having followed specialised training)  ▢ restrictions for onward transfers |

▢ other (please describe): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Supplementary measures implemented for transfer outside of the EEA or without an adequacy decision (“safe countries”):**

|  |  |
| --- | --- |
| ▢ SCCs for Controller directly with sub processors  ▢ BCRs  ▢ data centres inside the EEA  ▢ quick deletion protocols after transit | ▢ support access from outside of EEA or safe countries only upon active clearance  ▢ Automatic notification for access  ▢ encryption in transit  ▢ encryption in rest |

▢ other (please describe): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis) for example Continuous and daily basis.**

|  |  |
| --- | --- |
| ▢ continuously/ possibly daily  ▢ weekly | ▢ monthly  ▢ on demand occasionally |

▢ other (please describe): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

▢ will be deleted right after conducting the process (description see above)

OR

|  |  |
| --- | --- |
| ▢ 6 months  ▢ 1 year  ▢ 2 years  ▢ 3 years | period starts from:  ▢ from collection date  ▢ from finalising the intended data processing  ▢ annually from start of the cooperation |
| ▢ others (please describe and provide justification):  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |

1. **Processor’s Data Protection Contact Person** [if applicable]. In the event of a change of the contact person, the Processor will notify the Controller of this change in writing or in text form.

Name:

E-mail address:

Telephone number:

**APPENDIX 2 -** [**JURISDICTION SPECIFIC TERMS**](https://www.twilio.com/legal/data-protection-addendum#jurisdiction-specific-terms)

1. **Australia**
   1. The definition of “Applicable Data Protection Legislation” includes the Australian Privacy Principles and the Australian Privacy Act (1988).
   2. The definition of “Personal Data” includes “Personal Information” as defined under Applicable Data Protection Legislation.
2. **Brazil**
   1. The definition of “Applicable Data Protection Legislation” includes the Lei Geral de Proteção de Dados (LGPD).
   2. The definition of “Personal Data Breach” includes a security incident that may result in any relevant risk or damage to data subjects.
   3. The definition of “Processor” includes “operator” as defined under Applicable Data Protection Legislation.
3. **Canada**
   1. The definition of “Applicable Data Protection Legislation” includes the Federal Personal Information Protection and Electronic Documents Act (PIPEDA).
   2. Centric Software will implement technical and organizational measures as set forth in Appendix 4 of this DPA.
4. **European Economic Area (EEA)**
   1. The definition of “Applicable Data Protection Legislation” includes the General Data Protection Regulation (EU 2016/679) (“GDPR”).
5. **Israel**
   1. The definition of “Applicable Data Protection Legislation” includes the Protection of Privacy Law (PPL).
   2. The definition of “Controller” includes “Database Owner” as defined under Applicable Data Protection Legislation.
   3. The definition of “Processor” includes “Holder” as defined under Applicable Data Protection Legislation.
   4. Company will require that any personnel authorized to process Centric Personal Data comply with the principle of data secrecy and have been duly instructed about Applicable Data Protection Legislation. Such personnel sign confidentiality agreements with Company in accordance with Section 3 “Company’s Obligations” of this DPA.
   5. Company must take sufficient steps to ensure the privacy of data subjects by implementing and maintaining the security measures as specified in Appendix 4 of this DPA and complying with the terms of the Agreement.
   6. Company must ensure that the Centric Personal Data will not be transferred to an Onward Company unless such Onward Company has executed an agreement with the Company pursuant to Section 4 “Onward Sub-processing” of this DPA.
6. **Japan**

The definition of “Applicable Data Protection Legislation” includes the Act on the Protection of Personal Information (APPI).

1. **Mexico**

The definition of “Applicable Data Protection Legislation” includes the Federal Law for the Protection of Personal Data Held by Private Parties and its Regulations (FLPPIPPE).

1. **Singapore**
   1. The definition of “Applicable Data Protection Legislation” includes the Personal Data Protection Act 2012 (PDPA).
   2. Company will Process Centric Personal Data to a standard of protection in accordance with the PDPA by implementing adequate technical and organizational measures as set forth in Appendix 4 and complying with the terms of the Agreement.
2. **Switzerland**

The definition of “Applicable Data Protection Legislation” includes the Swiss Federal Data Protection Act of 19 June 1992 and its Ordinance 2012 (“Swiss FDPA”).

1. **United Kingdom (UK)**

The definition of “Applicable Data Protection Legislation” includes the UK Data Protection Legislation.

1. **United States of America** 
   1. “US State Privacy Laws” mean all state laws relating to the protection and processing of personal data in effect in the United States of America, which may include, without limitation, the California Consumer Privacy Act, as amended by the California Privacy Rights Act (“CCPA”), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, and the Utah Consumer Privacy Act.
   2. The definition of “Applicable Data Protection Law” includes US State Privacy Laws.
   3. The term “personal information”, as used in this Section 11.3, will have the meaning provided in the CCPA.

**APPENDIX 3 - INTERNATIONAL TRANSFER MECHANISM**

1. **Order of Precedence**

In the event the Services are covered by more than one Transfer Mechanism, the Transfer of Centric Personal Data will be subject to a single Transfer Mechanism in accordance with the following order of precedence: (a) the Standard Contractual Clauses as set forth in Section 2 “Standard Contractual Clauses or SCCs” below of this Appendix 3 ; (c) the UK Addendum as set forth in Section 4 “UK Transfers” below of this Appendix 3; and, if neither (a) nor (b) is applicable, then (c) other applicable data Transfer Mechanisms permitted under Applicable Data Protection Legislation.

1. **Standard Contractual Clauses or SCCs** (indicate which applies)

The Parties agree that the Standard Contractual Clauses will apply only to the Processing of Centric Personal Data Transferred from the EEA or Switzerland, either directly or via onward transfer, to any country or recipient outside the EEA or Switzerland to (i) any country that does not ensure an adequate level of data protection within the meaning of EU Data Protection Legislation (ii) to any recipient which is not subject to other binding obligations, code of conduct or certification as determined to be sufficient by the Supervisory Authority or (iii) any recipient not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for personal data, including but not limited to Binding Corporate Rules for Processors. For data transfer that are subject to the Standard Contractual Clauses, the Standard Contractual Clauses will be deemed entered into, and incorporated in this DPA by this reference, and completed as follows:

* Module 1 of the SCCs will apply where Centric Software is a Controller and Company is also a Controller of the Transferred Centric Personal Data;
* Module 2 of the SCCs will apply where Centric Software is a Controller and Company is a Processor of the Transferred Centric Personal Data;
* Module 3 of the SCCs will apply where Centric Software is a Processor and Company is a is also a Processor of the Transferred Centric Personal Data (i.e., Centric Software processes the Centric Personal Data on behalf of a third party Controller);

Whereby:

* Clause 7 “Docking clause” of the SCCs shall apply
* For Modules 2 and 3 only, in Clause 9 “Use of subprocessors” of the SCCs, Option 1 Specific Prior Authorisation shall apply. In the event that the Onward Company is located outside of the EEA, Company shall provide Centric Software with a documented data protection risk assessment relating to the transfer and processing of the Centric Personal Data intended by the Onward Company. Company will provide Centric Software with an updated **Appendix 5 “List of Permitted Onward Companies”** that reflects these changes.
* In Clause 11 “Redress” of the SCCs, the optional language shall apply;
* In Clause 17 “Governing Law”, Option 2 is selected.
* In Annex I,
  + Part A of the SCCs shall be completed with the parties names, contact details and activities set out or otherwise described in the Agreement and this DPA (with Centric Software acting as the Data Exporter and Company acting as the Data Importer) and execution of this DPA shall be deemed execution of the SCCs;
  + Part B of the SCCs shall be completed with the information set forth in **Appendix 1 “Details about Processing of Centric Personal Data”** of this DPA; and

1. ;
   * Part C of the SCCs: the supervisory authority with responsibility for ensuring compliance by the Data Exporter is as provided in Clause 13 of the SCCs.

* **Annex 4 “Technical and organizational measures to ensure the security of the data**” serves as Annex II of the SCCs.
* For Modules 2 and 3 only, Annex III shall be deemed completed with the list set out in **Appendix 5 “List of Permitted Onward Companies”**.

1. **Swiss Transfers**

To the extent that Centric Personal Data Transfers from Switzerland are subject to the Standard Contractual Clauses in accordance with Section 2 of this Appendix 3, the following amendments will apply to the Standard Contractual Clauses:

1. References to “Regulation (EU) 2016/679” shall be interpreted as references to the Swiss FDPA (as applicable);
2. References to specific Articles of “Regulation (EU) 2016/679” shall be replaced with the equivalent article or section of the Swiss FDPA (as applicable);
3. References to “EU”, “Union”, “Member State” and “Member State law” shall be replaced with references to the “Switzerland”, or “Swiss law” (as applicable);
4. The term “member state” shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., Switzerland);
5. Clause 13(a) and Part C of Annex I are not used and the “competent supervisory authority” is the Swiss Federal Data Protection Information Commissioner (as applicable);
6. References to the “competent supervisory authority” and “competent courts” shall be replaced with references to the “Swiss Federal Data Protection and Information Commissioner” and “applicable courts of Switzerland” (as applicable);
7. In Clause 17, the SCCs shall be governed by the laws of Switzerland; and with respect to transfers to which the Swiss FDPA applies,
8. Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland.
9. **UK Transfers**

Any conflict between the terms of the SCCs and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

Parties agree that the UK International Data Transfer Agreement will apply to Centric Personal Data that is transferred from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is not recognized by the competent United Kingdom regulatory authority or governmental body for the United Kingdom as providing an adequate level of protection for personal data. For data transfers from the United Kingdom that are subject to the UK Addendum, the UK Addendum will be deemed entered into, and incorporated into this DPA by this reference, and completed as follows:

1. In Table 1 of the UK Addendum, Customer's and Centric Software's details and key contact information are set forth in Section 2(e) of this Appendix 3;
2. In Table 2 of the UK Addendum, information about the version of the Approved EU SCCs, modules, and selected clauses, which the UK Addendum is appended to, are set forth in Section 2 “Standard Contractual Clauses or SCCs” of this Appendix 3;
3. In Table 3 of the UK Addendum:
4. The list of Parties is set forth in Section 2(e) of this Appendix 3;
5. The description of the transfer is set forth in **Appendix 1 “Details about Processing of Centric Personal Data”** of this DPA;
6. **Annex 4 “Technical and organizational measures to ensure the security of the data**” serves as Annex II of the UK Addendum
7. The list of sub-processors is set forth in Appendix 5 “List of authorized Sub-Processors”; and
8. In Table 4 of the UK Addendum, both the Importer and the exporter may end the UK Addendum in accordance with the terms of the UK Addendum.

**APPENDIX 4- TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE CENTRIC PERSONAL DATA**

[TO BE COMPLETED BY COMPANY]

*The GDPR and the security questionnaires can also be attached. In that case, the following sentence shall be added: “In case of conflict between the technical and organizational measures, provided by Centric Software below, and the GDPR and the security questionnaires, the latter shall prevail.”*

**EXPLANATORY NOTE:**

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

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

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

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 and, for transfers from a processor to a Company, to the data exporter

**APPENDIX 5 - LIST OF PERMITTED ONWARD COMPANIES**

[TO BE COMPLETED BY COMPANY]

**PART A – EEA BASED ONWARD COMPANINES**

1. **Permitted Onward Company A:** Company Name [Insert Legal name of Onward Company A]

* Details of this Onward Company: Registered office [Address/Country], Contact Information [email address/telephone number], Data Protection Officer [*if applicable*]
* Details of the Processing of Protected Data which may be undertaken by this Onward Company subject to and in accordance with this DPA:
  + Subject matter of the processing: [insert]
  + Duration of the processing: [insert]
  + Nature and purpose of the processing: [insert]
  + Geographical location of the processing by the sub-processor: [insert]
  + Type of Personal Data: [insert]
  + Categories of Data Subject: [insert]
  + Details of any further onward companies used to provide services under this Agreement: [insert]
  + List subject matter, nature and purpose of any further processing: services which may be processing personal data: [Insert]
  + Geographical location of the processing: [insert]

**PART B – NON-EEA ONWARD COMPANIES**

1. **Permitted Onward Company A:** Company Name [Insert Legal name of Onward Company A]

* Details of this Onward Company: Registered office [Address/Country], Contact Information [email address/telephone number], Data Protection Officer [*if applicable*]
* Details of the Processing of Protected Data which may be undertaken by this Onward Company subject to and in accordance with this DPA:
  + Subject matter of the processing: [insert]
  + Duration of the processing: [insert]
  + Nature and purpose of the processing: [insert]
  + Geographical location of the processing: [insert]
  + Type of Personal Data: [insert]
  + Categories of Data Subject: [insert]
  + Details of any further onward companies used to provide services under this DPA: [insert]
  + List subject matter, nature and purpose of any further processing: services which may be processing personal data: [Insert]
  + Geographical location of the processing: [insert

**APPENDIX 6 – TRANSFER IMPACT ASSESSMENT**

[TO BE COMPLETED BY COMPANY AND REVIEWED BY CENTRIC SOFTWARE]

This Transfer Impact Assessment must include:

1. the specific circumstances of the Transfer, the intended onward Transfers, the type of recipient, the purpose of Processing, the categories and format of the transferred Centric Personal Data, the economic sector in which the Transfer occurs, the storage location of the Centric Personal Data transferred;
2. the Legislation 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 Transfers and the applicable limitations and safeguards; and
3. any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under the Standard Contractual Clauses.