DATA PRIVACY TERMS FOR ACCENTURE SOFTWARE FOR HCM AND CLOUD ERP TOOLS SERVICES

These Data Privacy Terms apply to Client Personal Information processed by Accenture and its subprocessors on Client's behalf in connection with its provision/performance of the SaaS Services, Support and Maintenance or other professional services described in the related Service Order or Order Form for Accenture HCM Software and ERP Cloud Tools (the "Services").

Definitions

For the purposes of these Data Privacy Terms the following additional definitions shall apply. Capitalized terms not defined below shall have the meaning set forth in the applicable HCM and ERP Cloud Tools Service Order or Order Form.

"*Accenture EU Processor BCR*" means the Accenture's Binding Corporate Rules for Processors approved by the Irish Data Protection Commission (Supervisory Authority), and available at the following URL: https://www.accenture.com/us-en/about/binding-corporate-rules or any successor webpage.

"Data Privacy Laws" means all applicable data protection and privacy Laws that apply to the processing of personal data under a particular Service Order or Order Form, including, as applicable, General Data Protection Regulation 2016/679 (GDPR), new Federal Data Protection Act 2020 (Switzerland), UK Data Protection Act 2018 (DPA 2018) and UK General Data Protection Regulation (UK GDPR), and any US state or federal laws or regulations pertaining to the collection, use, disclosure, security or protection of personal data, or to security breach notification, e.g., California Consumer Privacy Act of 2018 ("CCPA"), as amended by the California Privacy Rights Act of 2020 ("CPRA").

"*EEA+*" for the purpose of these Data Privacy Terms means the European Economic Area consisting of any member states of the European Union, Iceland, Liechtenstein and Norway, as well as Switzerland.

"Information Security Incident" means a breach of Accenture's security leading to the accidental or unlawful destruction, loss, alteration or unauthorized acquisition, disclosure, misuse or access to Client Personal Information transmitted, stored or otherwise processed by Accenture."*Restricted Country*" means a country, a territory or one or more specified sectors within that country that do not benefit from an adequacy decision under the Data Protection Law applicable to the data exporter.

"*Transfer*" means the disclosure, sharing, transmission or otherwise making available for processing of Client Personal Information by a data exporter to a data importer based in another jurisdiction.

"*UK Addendum*" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses VERSION B1.0, issued by the Information Commissioner under S119A(1) Data Protection Act 2018, as amended from time to time.

***

Client shall be the controller of Client Personal Information, Accenture shall be the processor, and each Party shall comply with the relevant data privacy laws to the extent applicable to such Party in its respective role. Client warrants to Accenture that it has all necessary rights to provide the Client Personal Information to Accenture for the processing to be performed in relation to the Services. Client shall be responsible for and providing all necessary notices and, when applicable, obtaining all necessary consents from the concerned individuals, as required under the relevant Data Privacy Laws in relation to the processing of the Client Personal Information.

The Parties hereby acknowledge and agree to the following with respect to the processing of any Client Personal Information under these Data Privacy Terms:

1. Unless otherwise required by law, Accenture shall process Client Personal Information on Client's behalf as follows:

- **The subject matter of the processing** is limited to the Client Personal Information identified in this document.
- **The nature and purpose of the processing** shall be to provide the Services as defined in the description of the Services in the relevant Service Order or Order Form concluded between Client and Accenture.

- **The duration of the processing** is the Term of the related Service Order or Order Form.
- **The types of Client Personal Information** are name, phone numbers, e-mail address, time zone, address data, system access / usage / authorization data, company name, contract data (e.g. employment, contractors), and other data contained in Client's system of records.

  Client acknowledges that the following types of Personal Information cannot be entered by the Authorized Users into the SaaS Services or processed by Accenture while performing Services: Debit card number; Credit card number; Credit reports, credit scores and fraud alerts; Loan or deposit balances; Payment or purchase history (including information relevant to targeted marketing, e.g., product order history, service subscription history, descriptive listing of consumers); Medical care info, such as admissions, discharges, organ donations, medications, data pertaining to the health status of the data subject; this encompasses Protected Health Information as defined in 45 CFR 160.103 of the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA); Genetic Information; Biometric identifiers (DNA, finger, iris or retina recognition, facial recognition, hand geometry, ear, signature, and voice prints/speaker recognition technology, speaker verification or authentication); Geo-location information (GPS, Movement, GSP, Wifi, Bluetooth data); "Black Box" Data; e.g. telemetric, in-vehicle or in-home monitoring; Conversations (voice recordings, transcripts, or overheard); Political Views (affiliation or support with a political party or ideology); Criminal charges and convictions and court records.
- **The categories of data subjects**, unless otherwise provided in the applicable Service Order or Order Form, include employees, contractors, business partners or other individuals whose Personal Information is stored in the SaaS Services or in the Client's system of records.

2. Accenture will process Client Personal Information only in accordance with Client's documented instructions. These Data Privacy Terms and the applicable Service Order or Order Form for Accenture HCM and ERP Cloud Tools constitute such documented initial instructions. Accenture shall use reasonable efforts to follow any other Client's instructions as long as they are required by law, technically feasible and do not require changes to the Services. If Client requires that Accenture follow a processing instruction that may generate additional costs for Accenture, a mutually agreed change request to the Service Order, Order Form or GTC must be concluded in advance.

If Client requires that Accenture follow a processing instruction despite Accenture's notice that such instruction may, in Accenture's opinion, infringe an applicable Data Protection Law, Client shall be responsible for all liability, and shall defend, indemnify and hold Accenture harmless against all claims and damages, arising from any continued processing in accordance with such instruction.

3. Accenture shall: (i) not retain, use, disclose or otherwise process Client Personal Information for any purpose, including any commercial purpose, except as set forth in Section 2.; (ii) not "sell" or "share" (as each term is defined in CCPA, TDPSA, or other US Data Privacy Laws, as applicable) Client Personal Information; (iii) not process Client Personal Information outside the direct relationship between Accenture and Client, unless otherwise required by law; (iv) provide the same level of protection required by the relevant obligations under the applicable Data Privacy Laws for such Client Personal Information received by Accenture; (v) not combine Client Personal Information with any other personal data or personal information Accenture receives from, or on behalf of, another person or collects from its own interactions with individuals other than as part of providing the Services; (vi) notify Client of breach or if it can no longer meet its obligations under the applicable Data Privacy Laws and work with the Client to take appropriate steps to protect Client Personal Information; (vii) not attempt to deanonymize, reidentify or disaggregate any anonymized, pseudonymous or aggregated Client Personal Information. Client agrees that execution of these Data Privacy Terms by Accenture shall be deemed to constitute any certification that is required under applicable Data Privacy Laws to the restrictions on sale, retention, use, or disclosure of Client Personal Information herein.

4. All Accenture personnel, including subcontractors, authorized to process the Client Personal Information shall be subject to confidentiality obligations and/or subject to an appropriate statutory obligation of confidentiality.

5. Each Party shall implement appropriate technical and organizational security measures to safeguard Client Personal Information from unauthorized processing or accidental loss or damage within their own

respective environments (e.g., systems, networks, facilities) and such standards will govern and control in their respective environments. Accenture shall implement the measures further described in Accenture's client data safeguards accessible here: https://www.accenture.com/client-data-safeguards, all of which are designed to provide a level of security appropriate to the risk in respect of the processing of Client Personal Information. Client will enable Multi-Factor Authentication in its Successfactors systems. In addition to performing Services from Accenture locations, Accenture personnel may perform the Services or any portion of the Services remotely, provided that performing remotely does not (i) adversely impact Accenture's ability to perform its obligations under the relevant Service Order or Order Form; or (ii) require any increase to the applicable Fees.

For Services provided on a remote basis, any contractual requirements to provide physical and environmental security controls (e.g., secure bays; security guards; CCTV) at the Accenture service locations will not apply to remote work locations. In addition, where Accenture personnel are required to access Client systems from a remote work location, such access will only occur using Accenture devices.

6. Client generally authorizes the engagement of the Accenture's affiliates, Accenture's Cloud Vendor and the other third parties listed in the applicable Service Order or Order Form as subprocessors. Accenture shall contractually require (including via standard contractual clauses, sub-processing agreements or, with respect to Accenture's affiliates, intra-company agreements as applicable) any such subprocessors to comply with data protection obligations that are equivalent to those Accenture is required to comply with hereunder to the extent applicable to the subprocessors' subcontracted services. When applicable, any Transfers of Client Personal Information to third-party subprocessors ("Third Party Subprocessors") will be managed by Accenture in accordance with the applicable Data Privacy Laws, including by leveraging data transfer mechanisms executed by Accenture with the relevant third-party subprocessors at global level. Accenture shall remain fully liable for the performance of the subprocessors according to what provided for in the agreement with Client. Accenture shall provide Client with e-mail notification of any intended changes to the authorized subprocessors and Client shall promptly, and in any event within 10 business days, notify Accenture in writing of any reasonable objection to such changes. If Client raises such objections, the Parties shall discuss and resolve any disagreement via the dispute resolution procedure indicated in the GTC. If a resolution cannot be reached, Client will be only entitled to terminate the applicable Service Order or Order Form upon written notice to Accenture, provided that Client provides such notice within ninety (90) days from the end of the dispute resolution period indicated in the GTC.

7. Taking into account the nature of the Services and the information available to Accenture, Accenture shall cooperate with Client as reasonably requested to assist Client in complying with its obligations under the applicable Data Privacy Laws with respect to: (i) Client's implementation of appropriate security measures; (ii) Client's obligation to respond to requests from Client's data subjects; (iii) Client's obligation to notify regulators and data subjects of a personal data breach with respect to Client Personal Information as required by the applicable Data Privacy Laws; (iv) Client's obligation to conduct data protection impact assessments; and (v) Client's obligations to consult with regulators when so required by the applicable Data Privacy Laws.

8. Accenture shall maintain procedures to detect and respond to Information Security Incidents. If an Information Security Incident occurs which may reasonably compromise the security or privacy of Client Personal Information, Accenture will promptly notify Client without undue delay. Accenture will cooperate with Client in investigating the Information Security Incident and, taking into account the nature of the Services provided and the information available to Accenture, provide assistance to Client as reasonably requested with respect to Client's breach notification obligations under any applicable Data Privacy Laws.

9. Upon expiration or termination of the applicable Service Order or Order Form, Accenture **shall return or destroy** any Client Personal Information in accordance with Client's instruction. For clarity, Client Personal Information on Accenture's shared IT backup media will be erased within ninety (90) days pursuant to Accenture's internal policy.

10. Accenture shall make available to Client information reasonably requested by Client to demonstrate Accenture's compliance with its obligations in these Data Privacy Terms and Accenture shall submit to audits and inspections by Client (or Client directed third parties) in accordance with a process to be

mutually agreed to avoid disruption of the Services and protect the confidential information of Accenture, its authorized subprocessors and its other clients and in accordance with the following principles:

- audit limited to once a year;
- not to exceed 3 business days unless otherwise agreed by the parties in writing.
- reasonable prior written notice (at least 60 days unless a data protection authority requires Client's earlier control under mandatory Data Privacy Laws).
- scope and agenda of the audit to be determined in advance.

With regard to this section, Accenture shall inform Client if, in Accenture's opinion, any Client instruction infringes the applicable Data Privacy Law.

In the context of SaaS Services, Client acknowledges that Accenture's Third Party Subprocessors, such as the Cloud Vendor, use external, independent auditors to audit and verify the adequacy of their security measures, including the security of their physical data centers, and generate an audit report, available annually ("Report"). The Reports may be considered Third Party Subprocessors' Confidential Information and will be available to Client, at Client's request, subject to Client executing the Third Party Subprocessor's standard non-disclosure agreement, when applicable**.** Client agrees to exercise any right to conduct an audit or inspection of the Third Party Subprocessor, including under any applicable transfer mechanism , by instructing Accenture to obtain the relevant Third Party Subprocessor's Report, as described in this section. Client may change this instruction at any time upon written notice to Accenture, provided if the Third Party Subprocessor declines to submit to an audit or inspection requested by Client, Accenture will not be in breach of these Data Privacy Terms, but Client is entitled to terminate the related Service Order to which such request relates upon 30 days' notice to Accenture. Nothing in this Section is deemed to affect any supervisory authority's or data subject's rights under the applicable Data Privacy Laws.

11. Client acknowledges and agrees that to deliver the Services, Client Personal Information may be transferred outside of the country where such Personal Information originates from. In such a case, the following provisions shall apply:

11.1 Transfers of Client Personal Information from any EEA+ country

(a) Any Transfers of Client Personal Information from any EEA+ country to Accenture affiliates located in a Restricted Country shall be governed by the Accenture EU Processor BCR that are incorporated by reference herein and are an integral part of these Data Privacy Terms and the respective Service Order, Order Form and the GTC.

(b) Responsibilities of the parties.

(i) **Accenture as data exporter**. If the Accenture contracting entity is based within the EEA+, the Parties acknowledge and agree that Accenture shall be considered the data exporter, and the relevant Accenture affiliates shall be considered the data importers. Accenture shall be responsible for conducting any required transfer impact assessment.

(ii) **Client as data exporter**. If the Accenture contracting entity is based outside of the EEA+, the Parties acknowledge and agree that (1) Client and/or its relevant affiliates shall be considered the data exporter(s) and shall comply with the corresponding obligations under GDPR / the Swiss Data Protection Law, including conducting any required transfer impact assessment, and (2) Accenture / the relevant Accenture affiliates shall be considered the data importer(s) and shall comply with the corresponding obligations under GDPR / the Swiss Data Protection Law, including cooperating with the data exporter(s) in assessing the risks of the Transfers by providing a country transfer risk assessment for the relevant Restricted Countries.

(c) In any case, Client shall be responsible and commits to: (i) inform any applicable data subjects of the Transfers and the Accenture Processor EU BCR, that can be made available to the data subjects upon request together with a copy of these Data Privacy Terms upon redaction of any sensitive and confidential commercial information; and (ii) specifically inform the data subjects of the Restricted Countries of destination, if the Transfers involve special categories of personal data.

(d) If Client acts as a processor with respect to the Client Personal Information subject to the Transfer, Client represents and warrants that Client's processing instructions, including with respect to the Transfers from any EEA+ country, have been authorized by the applicable data controller(s). In such a case, Client shall enforce Accenture EU Processor BCR on behalf or for the benefit of the actual controller(s) of Client Personal Information, in accordance with these Data Privacy Terms and the respective Service Order, Order Form and the GTC.

(e) Parties further agree that any references to "Client Service Agreements" made in Accenture Processor EU BCR, shall be deemed as made to the respective Service Order, Order Form and the GTC. In accordance with the respective Service Order, Order Form and the GTC, Client shall have the right to enforce the Accenture Processor EU BCR against the Accenture group, including judicial remedies and the right to receive compensation.

11.2 Transfers of Client Personal Information from the UK. Any Transfers of Client Personal Information from the UK to an Accenture Affiliate located in a Restricted Country shall be governed by the UK Addendum. If the Accenture contracting entity is based in the UK, any Transfers of Client Personal Information from the UK to an Accenture affiliate located in a Restricted Country shall be governed by the UK Addendum incorporating the Module Three – Processor to Processor of the EU Standard Contractual Clauses between Accenture and the applicable Accenture affiliate(s). If the Accenture contracting entity is based outside of the UK, Client/Client affiliates acting as the data exporter(s), and Accenture / the applicable Accenture affiliate(s), acting as data importer(s), shall execute the UK Addendum incorporating the appropriate module of the EU Standard Contractual Clauses based on the Transfers occurring under the applicable Service Order or Order Form.

11.3 Transfers of Client Personal Information from countries outside the EEA+ and the UK. Subject to any provisions of Section 11.1 above, at Client's direction, the Accenture EU Processor BCR will govern any Transfers of Client Personal Information made by Client and/or a Client affiliate from any country outside the EEA+ and the UK to Accenture affiliates located in Restricted Countries, as detailed in the relevant Service Order or Order Form. If a different transfer mechanism is required under the Data Privacy Laws applicable to the relevant Client entity acting as data exporter, the Parties will work together expeditiously and in good faith to establish the appropriate transfer mechanism to be implemented.

11.4 Transfer Mechanism. In the event that the transfer mechanisms agreed by the Parties herein are amended, replaced, or cease to be authorized as a means to provide "adequate protection" with respect to Transfers of Client Personal Information, the Parties will work together expeditiously and in good faith to establish another valid transfer mechanism and/or implement supplementary measures as needed to establish appropriate safeguards for such Client Personal Information.

11.5 Data Privacy Laws. Any data transfer agreements (including but not limited to any Standard Contractual Clauses), that the parties or their affiliates may enter into in connection with the Services provided pursuant to a Service Order or Order Form and the GTC will be considered part of the respective Service Order, Order Form and the GTC and, without prejudice to the rights of any data subjects under any data transfer agreement, governed by the terms thereof.