DATA PRIVACY TERMS FOR ACCENTURE HCM 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 Services described in the related Service Order or Order Form.

In the context of SaaS Services, these Data Privacy Terms shall not apply to non-production environments if such environments are made available by Accenture (e.g. a test instance of the SaaS Services), and Client shall not store Client Personal Information in such environments.

Client shall be the controller of Client Personal Information, and Accenture shall be the processor of such data 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 Data to Accenture for the processing to be performed in relation to the Services. Client shall be responsible for obtaining all necessary consents, and providing all necessary notices, as required under the relevant Data Protection Laws in relation to the processing of the Client Personal Data.

The Parties hereby acknowledge and agree to the following with respect to the processing of any Client Personal Information under this Agreement:

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 Personal Information** are: name, phone numbers, e-mail address, time zone, address data, system access / usage / authorization data, company name, contract data, invoice data. 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)
  - Information regarding sexual life or sexual orientation
  - Political Views (affiliation or support with a political party or ideology)
  - Criminal charges and convictions and court records.
- **The categories of data subjects** are: unless provided otherwise by Client, will include employees, contractors, business partners or other individuals whose Personal Information is stored in the SaaS Services or in the Client's HR system of records.

2. Accenture will process Client Personal Information only in accordance with **Client's documented instructions**. These Data Privacy Terms 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 Agreement 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. 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.

4. Each Party shall implement appropriate **technical and organizational security measures** to safeguard Client Personal Information from unauthorized processing or accidental loss or damage. Client acknowledges and agrees that, taking into account the ongoing state of technological development, the costs of implementation and the nature, scope, context and purposes of the processing of the Client Personal Information, as well as the likelihood and severity of risk to individuals, Accenture's implementation of and compliance with the security measures set forth in **Attachment A** to this document provide a level of security appropriate to the risk in respect of the processing of the Client Personal Information.

5. Client specifically authorizes the engagement of Accenture's affiliates as **subprocessors** and generally authorizes, for the SaaS Services, the engagement of Accenture's Cloud Vendor SAP SE, as subprocessor. Accenture shall contractually require any such subprocessors to comply with data protection obligations that are at least as restrictive as those Accenture is required to comply with hereunder to the extent applicable to the subprocessors' subcontracted services. Accenture shall remain fully liable for the performance of the subprocessors. Accenture shall provide Client with written notice 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's objection is based on anything other than the proposed subprocessor's inability to comply with agreed data protection obligations, then any further adjustments shall be at Client's cost. Any disagreements between the Parties shall be resolved via the contract dispute resolution procedure.

6. Taking into account the nature of the processing and when the processing is within the scope of the EU General Data Protection Regulation ("GDPR") , Accenture shall provide assistance to Client as reasonably requested in responding to requests by data subjects to exercise the rights set out in Chapter III of the GDPR , including rights of access, rectification, erasure, portability, and the right to restrict or object to certain processing. Client shall be responsible for the reasonable costs of such assistance.

7. Taking into account the nature of the processing and the information available to Accenture, when the processing is within the scope of the GDPR Accenture shall provide reasonable assistance to Client with respect to: (i) Client's implementation of appropriate security measures; (ii) Client's obligation to notify regulators and data subjects of a breach with respect to Client Personal Information as required by GDPR; (iii) Client's obligation to conduct data protection impact assessments with respect to the processing as required by GDPR; and (iv) Client's obligations to consult with regulators as required by GDPR. Client shall be responsible for the reasonable costs of such assistance.

8. Upon expiration or termination of the Services, Accenture **shall return or destroy** any Client Personal Information in accordance with the Client instruction as soon as reasonably practicable and within a maximum period of 180 days.

9. 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 mutually agreed process designed 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 Protection Law).
- 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 any applicable Data Privacy Law.

In the context of SaaS Services, Client acknowledges that Accenture’s 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 are the Cloud Vendors’ Confidential Information and will be available to Client, at Client’s request, subject to Client executing the Cloud Vendor’s standard non-disclosure agreement**.** Client agrees to exercise any right to conduct an audit or inspection of the Cloud Vendor, including under the EU Model Clauses (defined here below) if applicable, by instructing Accenture to obtain the relevant Cloud Vendor’s Report, as described in this section. Client may change this instruction at any time upon written notice to Accenture, provided if the Cloud Vendor declines to submit to an audit or inspection requested by Client, Accenture will not be in breach of this Agreement, but Client is entitled to terminate the related Service Order to which such request relates upon 30 days’ notice to Accenture. If the EU Model Clauses apply, nothing in this section modifies the EU Model Clauses, and nothing in this Section affects any supervisory authority's or data subject's rights under the EU Model Clauses.

10. As of the Effective Date of the relevant Service Order or Order Form, **Client has identified for Accenture the countries where the data subjects originate**.

11. The Parties shall rely on the Standard Contractual Clauses for the Transfers of Personal Data to Processors Established in Third Countries, dated 5 February 2010 (2010/87/EU) as amended from time to time (the “EU Model Clauses”) to protect Client Personal Information being transferred from a country within the European Economic Area to a country outside the European Union or Switzerland not recognized by the European Commission as providing an adequate level of protection for Personal Information. Where the transfer relies on the EU Model Clauses, the Client, acting as data exporter, shall execute, or shall procure that the relevant Client entities execute, such EU Model Clauses with the relevant Accenture entity or a third-party entity, acting as a data importer.

Attachment A
Data Safeguards for Client Data

These data safeguards ("Data Safeguards") set forth the technical and organizational measures that Client and Accenture will follow with respect to maintaining the security of Client Data in connection with the Services described in the relevant Service Order or Order Form. In the event of a conflict between these Data Safeguards and any terms and conditions set forth in the Service Order or Order Form, the terms and conditions of these Data Safeguards shall prevail.
To the extent the Client Data includes Personal Data, and taking into account the ongoing state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of the Client Personal Data, as well as the likelihood and severity of risk to individuals, the implementation of and compliance with these Data Safeguards are designed to provide a level of security appropriate to the risk in respect of the processing of the Client Personal Data.

I. Controlling Standards

1. **Accenture Standards**. Accenture will maintain globally applicable policies, standards, and procedures intended to protect data within Accenture's environments, and, except as otherwise set forth herein, will comply with such policies in connection with the provision of the Services. Such policies will govern and control within Accenture's environments.

   Examples of such policies include:
   - System Security
   - Security of Information and Acceptable Use of Systems
   - Confidentiality
   - Data Privacy
   - Data Management

   Client and its Affiliates will comply with mutually agreed policies and standards, when relevant to the agreed services, and when accessing or operating within Accenture's environment.

2. **Client Standards**. Client and its Affiliates will maintain globally applicable policies, standards, and procedures intended to protect data within Client's and its Affiliates' environments, and, except as otherwise set forth herein, will comply with such policies in connection with the receipt and use of the Services. Such policies will govern and control within Client's and its Affiliates' environments.

   Examples of such policies include:
   - System Security
   - Security of Information and Acceptable Use of Systems
   - Confidentiality
   - Data Privacy
   - Data Management

   Accenture will comply with mutually agreed policies and standards, when relevant to the agreed services, and when accessing or operating within Client's or its Affiliates' environments.

II. Technical and Organizational Measures

Technical and Organizational Measures. Without limiting the generality of the foregoing, the Parties have implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Client Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction, as follows:

1. **Organization of Information Security**

   a) **Security Ownership.** Each Party will appoint one or more security officers responsible for coordinating and monitoring the security rules and procedures.

   b) **Security Roles and Responsibilities.** Each Party's personnel with access to Client Data will be subject to confidentiality obligations.

c) **Risk Management Program.** Each Party will have a risk management program in place to identify, assess and take appropriate actions with respect to risks related to the processing of the Client Data in connection with the applicable Agreement in place between the Parties.

2. **Asset Management**

a) **Asset Inventory.** Each Party will maintain an inventory of all media on which Client Data is stored. Access to the inventories of such media will be restricted to the Parties' personnel authorized in writing to have such access.

b) **Data Handling.**

i. Each Party will classify Client Data to help identify such data and to allow for access to it to be appropriately restricted (e.g., through encryption).

ii. Each Party will limit printing of Client Data to what is minimally necessary to perform services and have procedures for disposing of printed materials that contain Client Data.

iii. Each Party will require its personnel to obtain appropriate authorization prior to storing Client Data on portable devices, remotely accessing Client Data, or processing Client Data outside the Parties' facilities.

3. **Human Resources Security**

a) **Security Training.**

i. Each Party will inform its personnel about relevant security procedures and their respective roles. Each Party also will inform its personnel of possible consequences of breaching the security rules and procedures.

ii. Each Party will only use anonymous data in training.

4. **Physical and Environmental Security**

a) **Physical Access to Facilities.** Each Party will only allow authorized individuals to access facilities where information systems that process Client Data are located.

b) **Physical Access to Components.** Each Party will maintain records of the incoming and outgoing media containing Client Data, including the kind of media, the authorized sender/recipients, date and time, the number of media, and the types of Client Data they contain.

c) **Protection from Disruptions.** Each Party will use a variety of industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) systems to protect against loss of data due to power supply failure or line interference.

d) **Component Disposal.** Each Party will use industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) processes to delete Client Data when it is no longer needed.

5. **Communications and Operations Management**

a) **Operational Policy.** Each Party will maintain security documents describing their security measures and the relevant procedures and responsibilities of their personnel who have access to Client Data.

b) **Mobile Device Management (MDM).** Each Party will maintain a mobile device policy that:

i. Enforces device encryption;

ii. Protects and limits use of Client Data accessed or used on a mobile device; and

iii. Prohibits enrollment of mobile devices that have been "jail broken."

c) **Environments.** To the extent technically possible, the Parties will work together to limit the ability of Accenture personnel to access non-Client and non-Accenture environments from the Client systems.

d) Data Recovery Procedures

i. Each Party will have specific data recovery procedures in place designed to enable the recovery of Client Data being maintained in its systems.

ii. Each Party will review its data recovery procedures at least annually.

iii. Each Party will log data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.

e) Malicious Software. Each Party will have anti-malware controls to help avoid malicious software gaining unauthorized access to Client Data, including malicious software originating from public networks.

f) Data Beyond Boundaries.

i. Each Party will encrypt Client Data that is transmitted over public networks.

ii. Each Party will implement Multi-Factor Authentication for remote access over virtual private network (VPN).

iii. Each Party will protect Client Data in media leaving their facilities (e.g., through encryption).

g) Event Logging.

i. Each Party will log the use of their respective data-processing systems.

ii. Each Party will log access and use of information systems containing Client Data, including at a minimum registering the access ID, time, and authorization granted or denied.

6. Access Control

a) Access Policy. Each Party will maintain a record of security privileges of individuals having access to Client Data.

b) Access Authorization.

i. Each Party will maintain and update a record of personnel authorized to access Client Data via that Party's systems.

ii. When responsible for access provisioning, each Party will promptly provision authentication credentials.

iii. Each Party will deactivate authentication credentials where such credentials have not been used for a period of time (such period of non-use not to exceed six months).

iv. Each Party will deactivate authentication credentials upon notification that access is no longer needed (e.g. employee termination, project reassignment, etc.) within two business days.

v. Each Party will identify those personnel who may grant, alter or cancel authorized access to data and resources.

vi. Each Party will ensure that where more than one individual has access to systems containing Client Data, the individuals have unique identifiers/log-ins.

c) Least Privilege.

i. Technical support personnel will only be permitted to have access to Client Data when needed.

ii. Each Party will restrict access to Client Data to only those individuals who require such access to perform their job function.

iii. Each Party will limit access to Client Data to only that data minimally necessary to perform the services.

d) Integrity and Confidentiality. Each Party will instruct its personnel to disable administrative sessions when leaving premises or when computers are otherwise left unattended.

e) Authentication.

i. Each Party will use industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) practices to identify and authenticate users who attempt to access information systems.

ii. Where authentication mechanisms are based on passwords, each Party will require that the passwords are renewed regularly.

iii. Where authentication mechanisms are based on passwords, each Party will require the password to be at least eight characters long.

iv. Each Party will ensure that de-activated or expired identifiers are not granted to other individuals.

v. Each Party will monitor repeated attempts to gain access to information systems using an invalid password.

vi. Each Party will maintain industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

vii. Each Party will use industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, as well as during storage.

f) Network Design. Each Party will have controls to avoid individuals gaining unauthorized access to Client Data.

7. Patch Management

a) Each Party will have a patch management procedure that deploys security patches for systems used to process Client Data that includes:

i. Defined time allowed to implement patches (not to exceed 90 days for all patches); and

ii. Established process to handle emergency patches in a shorter time frame.

b) Each Party agrees that no software or hardware that is past its End of Life (EOL) will be used in the scope of services without a mutually agreed risk management process for such items.

8. Workstations

a) Each Party will implement controls for all workstations it provides that are used in connection with service delivery/receipt incorporating the following:

i. Encrypted hard drive

ii. Software agent that manages overall compliance of workstation and reports a minimum on a monthly basis to a central server

iii. Patching process to ensure workstations are current on all required patches

iv. Ability to prevent certain types of software from being installed (e.g. peer-to-peer software)

v. Antivirus with a minimum weekly scan

vi. Firewalls installed

vii. Data Loss Prevention tool (subject to any legal requirements, e.g. Works Council)

viii. Web filtering

9. Information Security Breach Management

a) Security Breach Response Process. Each Party will maintain a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the process for recovering data.

b) Service Monitoring. Each Party's security personnel will review logs as part of their security breach response process to propose remediation efforts if necessary.

10. Business Continuity Management

a) Each Party will maintain emergency and contingency plans for the facilities in which the Parties' information systems that process Client Data are located.

b) Each Party's redundant storage and procedures for recovering data will be designed to reconstruct Client Data stored by a Party in its original state from before the time it was lost or destroyed.