

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

TÉRMINOS DE PRIVACIDAD DE DATOS PARA LOS SERVICIOS DE ACCENTURE SOFTWARE PARA HCM Y HERRAMIENTAS ERP EN LA NUBE

Estos Términos de Privacidad de Datos se aplican a la Información Personal del Cliente tratada por Accenture y sus subencargados del tratamiento por cuenta del Cliente en relación con la prestación/ejecución de los Servicios SaaS, Soporte y Mantenimiento u otros servicios profesionales descritos en la Orden de Servicio u Orden de Pedido correspondiente para Accenture HCM Software y ERP Cloud Tools (los "Servicios").

Definiciones

A los efectos de estos Términos de Privacidad de Datos, se aplicarán las siguientes definiciones adicionales. Los términos en mayúscula no definidos a continuación tendrán el significado establecido en la Orden de Servicio u Orden de Pedido aplicable para HCM y ERP Cloud Tools.

"*BCR de Accenture para Encargados del Tratamiento en la UE*" significa las Normas Corporativas Vinculantes de Accenture para Encargados del Tratamiento aprobadas por la Comisión de Protección de Datos de Irlanda (Autoridad de Control), disponibles en la siguiente URL: <https://www.accenture.com/us-en/about/binding-corporate-rules> o cualquier página web sucesora.

"*Leyes de Privacidad de Datos*" significa todas las leyes aplicables de protección de datos y privacidad que se apliquen al tratamiento de datos personales en virtud de una Orden de Servicio u Orden de Pedido concreta, incluidas, según corresponda, el Reglamento General de Protección de Datos 2016/679 (RGPD), la nueva Ley Federal de Protección de Datos 2020 (Suiza), la Ley de Protección de Datos del Reino Unido de 2018 (DPA 2018) y el Reglamento General de Protección de Datos del Reino Unido (UK GDPR), y cualesquiera leyes o reglamentos estatales o federales de EE. UU. relativos a la recopilación, uso, divulgación, seguridad o protección de datos personales, o a la notificación de violaciones de seguridad, por ejemplo, la California Consumer Privacy Act de 2018 ("CCPA"), modificada por la California Privacy Rights Act de 2020 ("CPRA").

"*EEE+*" a los efectos de estos Términos de Privacidad de Datos significa el Espacio Económico Europeo, compuesto por los Estados miembros de la Unión Europea, Islandia, Liechtenstein y Noruega, así como Suiza.

"*Incidente de Seguridad de la Información*" significa una vulneración de la seguridad de Accenture que dé lugar a la destrucción, pérdida, alteración o adquisición, divulgación, uso indebido o acceso no autorizado, accidental o ilícito, de la Información Personal del Cliente transmitida, almacenada o tratada de otro modo por Accenture.

"*País Restringido*" significa un país, territorio o uno o más sectores específicos dentro de dicho país que no se benefician de una decisión de adecuación conforme a la

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

Ley de Protección de Datos aplicable al exportador de datos.

“*Transferencia*” significa la divulgación, intercambio, transmisión o puesta a disposición de otro modo para el tratamiento de la Información Personal del Cliente por un exportador de datos a un importador de datos ubicado en otra jurisdicción.

“*Anexo del Reino Unido*” significa el Anexo Internacional de Transferencia de Datos a las Cláusulas Contractuales Tipo de la Comisión Europea VERSIÓN B1.0, emitido por el *Information Commissioner* en virtud del artículo S119A(1) de la Data Protection Act 2018, según sea modificado ocasionalmente.

El Cliente será el controlante de la Información Personal del Cliente, Accenture será el encargado del tratamiento, y cada Parte cumplirá las leyes de privacidad de datos pertinentes en la medida en que sean aplicables a dicha Parte en su respectivo rol. El Cliente garantiza a Accenture que cuenta con todos los derechos necesarios para proporcionar la Información Personal del Cliente a Accenture para el tratamiento que se realizará en relación con los Servicios. El Cliente será responsable de proporcionar todos los avisos necesarios y, cuando corresponda, obtener todos los consentimientos necesarios de las personas afectadas, según lo exijan las Leyes de Privacidad de Datos pertinentes en relación con el tratamiento de la Información Personal del Cliente.

Las Partes reconocen y acuerdan lo siguiente respecto del tratamiento de cualquier Información Personal del Cliente conforme a estos Términos de Privacidad de Datos:

1. Salvo que la ley exija lo contrario, Accenture tratará la Información Personal del Cliente por cuenta del Cliente de la siguiente manera:
 - **El objeto del tratamiento** se limita a la Información Personal del Cliente identificada en este documento.
 - **La naturaleza y finalidad del tratamiento** será prestar los Servicios según se definen en la descripción de los Servicios de la Orden de Servicio u Orden de Pedido pertinente celebrada entre el Cliente y Accenture.
 - **La duración del tratamiento** es el Plazo de la Orden de Servicio u Orden de Pedido correspondiente.
 - **Los tipos de Información Personal del Cliente** son nombre, números de teléfono, dirección de correo electrónico, zona horaria, datos de dirección, datos de acceso/uso/autorización del sistema, nombre de la empresa, datos contractuales (por ejemplo, empleo, contratistas) y otros datos contenidos en el sistema de registros del Cliente.

El Cliente reconoce que los siguientes tipos de Información Personal no pueden ser ingresados por los Usuarios Autorizados en los Servicios SaaS ni tratados por Accenture al prestar los Servicios:

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.

número de tarjeta de débito; número de tarjeta de crédito; informes crediticios, puntajes crediticios y alertas de fraude; saldos de préstamos o depósitos; historial de pagos o compras (incluida la información relevante para marketing dirigido, por ejemplo, historial de pedidos de productos, historial de suscripción a servicios, listado descriptivo de consumidores); información de atención médica, como admisiones, altas, donaciones de órganos, medicamentos, datos relativos al estado de salud del titular de los datos; esto incluye la Información de Salud Protegida según se define en 45 CFR 160.103 de la Health Insurance Portability and Accountability Act de 1996 de EE. UU. (HIPAA); información genética; identificadores biométricos (ADN, reconocimiento de dedo, iris o retina, reconocimiento facial, geometría de la mano, oreja, firma y huellas de voz/tecnología de reconocimiento de hablante, verificación o autenticación de hablante); información de geolocalización (GPS, movimiento, GSP, Wifi, datos Bluetooth); datos de "caja negra", por ejemplo, telemétricos, monitoreo en vehículos o en el hogar; conversaciones (grabaciones de voz, transcripciones o conversaciones escuchadas); opiniones políticas (afiliación o apoyo a un partido político o ideología); cargos y condenas penales y antecedentes judiciales.

- **Las categorías de titulares de datos**, salvo que se disponga lo contrario en la Orden de Servicio u Orden de Pedido aplicable, incluyen empleados, contratistas, socios comerciales u otras personas cuya Información Personal se almacene en los Servicios SaaS o en el sistema de registros del Cliente.

2. Accenture tratará la Información Personal del Cliente únicamente de conformidad con las instrucciones documentadas del Cliente. Estos Términos de Privacidad de Datos y la Orden de Servicio u Orden de Pedido aplicable para Accenture HCM y ERP Cloud Tools constituyen dichas instrucciones iniciales documentadas. Accenture realizará esfuerzos razonables para seguir cualquier otra instrucción del Cliente siempre que sea exigida por la ley, técnicamente viable y no requiera cambios en los Servicios. Si el Cliente requiere que Accenture siga una instrucción de tratamiento que pueda generar costos adicionales para Accenture, deberá celebrarse previamente una solicitud de cambio mutuamente acordada a la Orden de Servicio, Orden de Pedido o TCG.

Si el Cliente requiere que Accenture siga una instrucción de tratamiento pese al aviso de Accenture de que dicha instrucción puede, a juicio de Accenture, infringir una Ley de Protección de Datos aplicable, el Cliente asume toda responsabilidad, y defenderá, indemnizará y mantendrá indemne a Accenture frente a todas las reclamaciones y daños derivados de cualquier tratamiento continuado conforme a dicha instrucción.

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

3. Accenture se obliga a: (i) no conservar, usar, divulgar ni tratar de otro modo la Información Personal del Cliente para ningún fin, incluido cualquier fin comercial, salvo lo establecido en la Sección 2; (ii) no “vender” ni “compartir” (según se define cada término en la CCPA, TDPSA u otras Leyes de Privacidad de Datos de EE. UU., según corresponda) la Información Personal del Cliente; (iii) no tratar la Información Personal del Cliente fuera de la relación directa entre Accenture y el Cliente, salvo que la ley exija lo contrario; (iv) proporcionar el mismo nivel de protección exigido por las obligaciones pertinentes conforme a las Leyes de Privacidad de Datos aplicables respecto de dicha Información Personal del Cliente recibida por Accenture; (v) no combinar la Información Personal del Cliente con otros datos personales o información personal que Accenture reciba de, o por cuenta de, otra persona o recopile de sus propias interacciones con personas, salvo como parte de la prestación de los Servicios; (vi) notificar al Cliente de cualquier incumplimiento o si ya no puede cumplir sus obligaciones conforme a las Leyes de Privacidad de Datos aplicables, trabajar con el Cliente para adoptar medidas adecuadas para proteger la Información Personal del Cliente; (vii) no intentar desanonimizar, reidentificar o desagregar ninguna Información Personal del Cliente anonimizada, seudonimizada o agregada. El Cliente acepta que la firma de estos Términos de Privacidad de Datos por Accenture se considerará como cualquier certificación requerida por las Leyes de Privacidad de Datos aplicables respecto de las restricciones de venta, conservación, uso o divulgación de la Información Personal del Cliente aquí previstas.

4. Todo el personal de Accenture, incluidos los subcontratistas, autorizados para tratar la Información Personal del Cliente estará sujeto a obligaciones de confidencialidad y/o a una obligación legal de confidencialidad adecuada.

5. Cada Parte implementará medidas técnicas y organizativas de seguridad adecuadas para proteger la Información Personal del Cliente contra el tratamiento no autorizado o la pérdida o daño accidental dentro de sus respectivos entornos (por ejemplo, sistemas, redes, instalaciones), y dichos estándares regirán y prevalecerán en sus respectivos entornos. Accenture implementará las medidas descritas adicionalmente en las salvaguardas de datos de clientes de Accenture disponibles aquí: <https://www.accenture.com/client-data-safeguards>, todas las cuales están diseñadas para proporcionar un nivel de seguridad adecuado al riesgo respecto del tratamiento de la Información Personal del Cliente. El Cliente habilitará la autenticación multifactor en sus sistemas SuccessFactors. Además de prestar los Servicios desde ubicaciones de Accenture, el personal de Accenture podrá prestar los Servicios o cualquier parte de ellos de forma remota, siempre que dicha prestación remota no (i) afecte negativamente la capacidad de Accenture para cumplir sus obligaciones conforme a la

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

Orden de Servicio u Orden de Pedido correspondiente; ni (ii) requiera aumento alguno de las Tarifas aplicables.

Para los Servicios prestados de forma remota, no se aplicarán a los lugares de trabajo remoto los requisitos contractuales de proporcionar controles de seguridad física y ambiental (por ejemplo, áreas seguras; guardias de seguridad; CCTV) en las ubicaciones de servicio de Accenture. Además, cuando el personal de Accenture deba acceder a los sistemas del Cliente desde un lugar de trabajo remoto, dicho acceso se realizará únicamente mediante dispositivos de Accenture.

6. El Cliente autoriza de forma general la contratación de las afiliadas de Accenture, el Proveedor Cloud de Accenture y los demás terceros enumerados en la Orden de Servicio u Orden de Pedido aplicable como subencargados del tratamiento. Accenture exigirá contractualmente (incluidas cláusulas contractuales tipo, acuerdos de subtratamiento o, respecto de las afiliadas de Accenture, acuerdos intragrupo, según corresponda) que dichos subencargados cumplan obligaciones de protección de datos equivalentes a aquellas que Accenture debe cumplir conforme al presente, en la medida aplicable a los servicios subcontratados por los subencargados. Cuando corresponda, cualquier Transferencia de Información Personal del Cliente a subencargados terceros ("Subencargados Terceros") será gestionada por Accenture de conformidad con las Leyes de Privacidad de Datos aplicables, incluso mediante mecanismos de transferencia de datos ejecutados por Accenture con los Subencargados Terceros pertinentes a nivel global. Accenture seguirá siendo plenamente responsable por el desempeño de los subencargados conforme a lo previsto en el acuerdo con el Cliente. Accenture notificará al Cliente por correo electrónico cualquier cambio previsto en los subencargados autorizados, y el Cliente notificará prontamente a Accenture por escrito, y en todo caso dentro de los 10 días hábiles, cualquier objeción razonable a dichos cambios. Si el Cliente formula dichas objeciones, las Partes discutirán y resolverán cualquier desacuerdo mediante el procedimiento de resolución de disputas indicado en las TGC. Si no se alcanza una resolución, el Cliente solo tendrá derecho a rescindir la Orden de Servicio u Orden de Pedido aplicable mediante notificación escrita a Accenture, siempre que el Cliente proporcione dicha notificación dentro de los noventa (90) días desde la finalización del período de resolución de disputas indicado en las TGC.

7. Teniendo en cuenta la naturaleza de los Servicios y la información disponible para Accenture, Accenture cooperará con el Cliente según se le solicite razonablemente para asistir al Cliente en el cumplimiento de sus obligaciones conforme a las Leyes de Privacidad de Datos aplicables respecto de: (i) la implementación por parte del Cliente de medidas de seguridad adecuadas; (ii) la obligación del Cliente de responder a solicitudes de los titulares de datos del

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

Cliente; (iii) la obligación del Cliente de notificar a reguladores y titulares de datos una violación de datos personales respecto de la Información Personal del Cliente según lo exijan las Leyes de Privacidad de Datos aplicables; (iv) la obligación del Cliente de realizar evaluaciones de impacto en protección de datos; y (v) las obligaciones del Cliente de consultar con reguladores cuando así lo exijan las Leyes de Privacidad de Datos aplicables.

8. Accenture mantendrá procedimientos para detectar y responder a Incidentes de Seguridad de la Información. Si ocurre un Incidente de Seguridad de la Información que pueda comprometer razonablemente la seguridad o privacidad de la Información Personal del Cliente, Accenture notificará prontamente al Cliente sin dilación indebida. Accenture cooperará con el Cliente en la investigación del Incidente de Seguridad de la Información y, teniendo en cuenta la naturaleza de los Servicios prestados y la información disponible para Accenture, brindará asistencia al Cliente según se solicite razonablemente respecto de las obligaciones del Cliente en cuanto a notificación de brechas de seguridad conforme a cualquier Ley de Privacidad de Datos aplicable.
9. Al vencimiento o terminación de la Orden de Servicio u Orden de Pedido aplicable, Accenture **devolverá o destruirá** cualquier Información Personal del Cliente de conformidad con las instrucciones del Cliente. Para mayor claridad, la Información Personal del Cliente en medios de respaldo de TI compartidos de Accenture será eliminada dentro de los noventa (90) días conforme a la política interna de Accenture.
10. Accenture pondrá a disposición del Cliente la información razonablemente solicitada por el Cliente para demostrar el cumplimiento por parte de Accenture de sus obligaciones en estos Términos de Privacidad de Datos, y Accenture se someterá a auditorías e inspecciones por parte del Cliente (o terceros indicados por el Cliente) de conformidad con un proceso que se acordará mutuamente para evitar la interrupción de los Servicios y proteger la información confidencial de Accenture, sus subencargados autorizados y sus demás clientes, y de acuerdo con los siguientes principios:
 - auditoría limitada a una vez al año;
 - no excederá de 3 días hábiles, salvo acuerdo escrito en contrario de las partes;
 - notificación escrita previa razonable (al menos 60 días, salvo que una autoridad de protección de datos requiera un control anterior del Cliente conforme a Leyes de Privacidad de Datos imperativas);
 - alcance y agenda de la auditoría determinados por adelantado.

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.

Respecto de esta sección, Accenture informará al Cliente si, a juicio de Accenture, alguna instrucción del Cliente infringe la Ley de Privacidad de Datos aplicable.

En el contexto de los Servicios SaaS, el Cliente reconoce que los Subencargados Terceros de Accenture, como el Proveedor Cloud, utilizan auditores externos e independientes para auditar y verificar la adecuación de sus medidas de seguridad, incluida la seguridad de sus centros de datos físicos, y generan un informe de auditoría, disponible anualmente ("Informe"). Los Informes podrán considerarse Información Confidencial de los Subencargados Terceros y estarán disponibles para el Cliente, a solicitud del Cliente, sujeto a que el Cliente suscriba el acuerdo estándar de confidencialidad del Subencargado Tercero, cuando corresponda. El Cliente acepta ejercer cualquier derecho a realizar una auditoría o inspección del Subencargado Tercero, incluso conforme a cualquier mecanismo de transferencia aplicable, instruyendo a Accenture para que obtenga el Informe correspondiente del Subencargado Tercero, según se describe en esta sección. El Cliente podrá modificar esta instrucción en cualquier momento mediante notificación escrita a Accenture, siempre que, si el Subencargado Tercero se niega a someterse a una auditoría o inspección solicitada por el Cliente, Accenture no estará en incumplimiento de estos Términos de Privacidad de Datos, pero el Cliente tendrá derecho a rescindir la Orden de Servicio relacionada a la que se refiera dicha solicitud mediante notificación con 30 días de antelación a Accenture. Nada en esta Sección se considerará que afecta los derechos de cualquier autoridad de control o titular de datos conforme a las Leyes de Privacidad de Datos aplicables.

11. El Cliente reconoce y acepta que, para prestar los Servicios, la Información Personal del Cliente podrá transferirse fuera del país del que dicha Información Personal proviene. En tal caso, se aplicarán las siguientes disposiciones:

11.1 Transferencias de Información Personal del Cliente desde cualquier país del EEE+

(a) Cualquier Transferencia de Información Personal del Cliente desde cualquier país del EEE+ a afiliadas de Accenture ubicadas en un País Restringido se regirá por las BCR de Accenture para Encargados del Tratamiento en la UE, que se incorporan al presente por referencia y forman parte integral de estos Términos de Privacidad de Datos y de la respectiva Orden de Servicio, Orden de Pedido y las TGC.

(b) Responsabilidades de las partes.

(i) **Accenture como exportador de datos.** Si la entidad contratante de Accenture está establecida dentro del EEE+, las Partes reconocen y acuerdan que Accenture será considerada el exportador de datos, y las afiliadas pertinentes de Accenture serán consideradas los importadores de datos.

(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

Accenture será responsable de realizar cualquier evaluación de impacto de transferencia requerida.

(ii) **Cliente como exportador de datos.** Si la entidad contratante de Accenture está establecida fuera del EEE+, las Partes reconocen y acuerdan que (1) el Cliente y/o sus afiliadas pertinentes serán considerados el/los exportador(es) de datos y cumplirán las obligaciones correspondientes conforme al RGPD / la Ley Suiza de Protección de Datos, incluida la realización de cualquier evaluación de impacto de transferencia requerida, y (2) Accenture / las afiliadas pertinentes de Accenture serán consideradas el/los importador(es) de datos y cumplirán las obligaciones correspondientes conforme al RGPD / la Ley Suiza de Protección de Datos, incluida la cooperación con el/los exportador(es) de datos en la evaluación de los riesgos de las Transferencias mediante la provisión de una evaluación de riesgo de transferencia de país para los Países Restringidos pertinentes.

(c) En cualquier caso, el Cliente será responsable y se compromete a: (i) informar a los titulares de datos aplicables de las Transferencias y de las BCR de Accenture para Encargados del Tratamiento en la UE, que podrán ponerse a disposición de los titulares de datos previa solicitud junto con una copia de estos Términos de Privacidad de Datos previa supresión de cualquier información comercial sensible y confidencial; y (ii) informar específicamente a los titulares de datos de los Países Restringidos de destino, si las Transferencias involucran categorías especiales de datos personales.

(d) Si el Cliente actúa como encargado del tratamiento respecto de la Información Personal del Cliente sujeta a la Transferencia, el Cliente declara y garantiza que las instrucciones de tratamiento del Cliente, incluidas las relativas a las Transferencias desde cualquier país del EEE+, han sido autorizadas por el/los responsable(s) del tratamiento aplicable(s). En tal caso, el Cliente hará valer las BCR de Accenture para Encargados del Tratamiento en la UE en nombre o en beneficio del/los responsable(s) real(es) del tratamiento de la Información Personal del Cliente, de conformidad con estos Términos de Privacidad de Datos y la respectiva Orden de Servicio, Orden de Pedido y las CGC.

(e) Las Partes acuerdan además que cualquier referencia a "Acuerdos de Servicios con Clientes" realizada en las BCR de Accenture para Encargados del Tratamiento en la UE se considerará efectuada a la respectiva Orden de Servicio, Orden de Pedido y las TGC. De conformidad con la respectiva Orden de Servicio, Orden de Pedido y las TGC, el Cliente tendrá derecho a hacer valer las BCR de Accenture para Encargados del Tratamiento en la UE contra el grupo Accenture, incluidos los recursos judiciales y el derecho a recibir compensación.

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

11.2 Transferencias de Información Personal del Cliente desde el Reino Unido. Cualquier Transferencia de Información Personal del Cliente desde el Reino Unido a una Afiliada de Accenture ubicada en un País Restringido se registrará por el Anexo del Reino Unido. Si la entidad contratante de Accenture está establecida en el Reino Unido, cualquier Transferencia de Información Personal del Cliente desde el Reino Unido a una afiliada de Accenture ubicada en un País Restringido se registrará por el Anexo del Reino Unido que incorpora el Módulo Tres - Encargado a Encargado de las Cláusulas Contractuales Tipo de la UE entre Accenture y la(s) afiliada(s) de Accenture aplicable(s). Si la entidad contratante de Accenture está establecida fuera del Reino Unido, el Cliente/las afiliadas del Cliente que actúen como exportador(es) de datos, y Accenture / la(s) afiliada(s) de Accenture aplicable(s), que actúen como importador(es) de datos, ejecutarán el Anexo del Reino Unido incorporando el módulo apropiado de las Cláusulas Contractuales Tipo de la UE en función de las Transferencias que ocurran en virtud de la Orden de Servicio u Orden de Pedido aplicable.

11.3 Transferencias de Información Personal del Cliente desde países fuera del EEE+ y del Reino Unido. Sujeto a cualquier disposición de la Sección 11.1 anterior, por instrucción del Cliente, las BCR de Accenture para Encargados del Tratamiento en la UE registrarán cualquier Transferencia de Información Personal del Cliente realizada por el Cliente y/o una afiliada del Cliente desde cualquier país fuera del EEE+ y del Reino Unido a afiliadas de Accenture ubicadas en Países Restringidos, según se detalle en la Orden de Servicio u Orden de Pedido pertinente. Si se requiere un mecanismo de transferencia diferente conforme a las Leyes de Privacidad de Datos aplicables a la entidad del Cliente pertinente que actúe como exportador de datos, las Partes trabajarán conjuntamente de manera expedita y de buena fe para establecer el mecanismo de transferencia adecuado que deberá implementarse.

11.4 Mecanismo de Transferencia. En caso de que los mecanismos de transferencia acordados por las Partes en el presente sean modificados, reemplazados o dejen de estar autorizados como medio para proporcionar "protección adecuada" respecto de las Transferencias de Información Personal del Cliente, las Partes trabajarán conjuntamente de manera expedita y de buena fe para establecer otro mecanismo de transferencia válido y/o implementar medidas complementarias según sea necesario para establecer salvaguardas apropiadas para dicha Información Personal del Cliente.

11.5 Leyes de Privacidad de Datos. Cualquier acuerdo de transferencia de datos (incluidas, entre otras, cualesquiera Cláusulas Contractuales Tipo) que las partes o sus afiliadas puedan celebrar en relación con los Servicios prestados conforme a una Orden de Servicio u Orden de Pedido y las CGC se considerará parte de la respectiva Orden de Servicio, Orden de

GTC and, without prejudice to the rights of any data subjects under any data transfer agreement, governed by the terms thereof.

Pedido y las CGC y, sin perjuicio de los derechos de cualesquiera titulares de datos conforme a cualquier acuerdo de transferencia de datos, se regirá por sus términos.