

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").

TERMOS DE PRIVACIDADE DE DADOS RELATIVOS AOS SERVIÇOS DE SOFTWARE PARA HCM E FERRAMENTAS DE ERP NA NUVEM DA ACCENTURE

Os presentes Termos de Privacidade de Dados aplicam-se às Informações Pessoais do Cliente tratadas pela Accenture e pelos seus subcontratantes ulteriores em nome do Cliente, no âmbito da prestação/execução dos Serviços SaaS, de Apoio e Manutenção ou de outros serviços profissionais descritos na Ordem de Serviço ou no Formulário de Encomenda correspondentes relativos ao Software para HCM e às Ferramentas de ERP na Nuvem da Accenture (os "Serviços").

Definições

Para efeitos dos presentes Termos de Privacidade de Dados, aplicam-se as seguintes definições complementares. Os termos em maiúsculas que não sejam definidos a seguir terão o significado estabelecido na Ordem de Serviço ou no Formulário de Encomenda aplicável das Ferramentas de HCM e ERP na Nuvem.

"BCR de Subcontratante da UE da Accenture" significa as Regras Corporativas Vinculativas da Accenture para Subcontratantes aprovadas pela Comissão Irlandesa de Proteção de Dados (Autoridade de Controlo) e disponíveis no seguinte URL: <https://www.accenture.com/us-en/about/binding-corporate-rules> ou qualquer página que lhe suceder.

"Leis de Privacidade de Dados" significa todas as Leis aplicáveis em matéria de proteção e privacidade de dados que se aplicam ao tratamento de dados pessoais no âmbito de uma determinada Ordem de Serviço ou Formulário de Encomenda, incluindo, conforme aplicável, o Regulamento Geral sobre a Proteção de Dados 2016/679 (RGPD), a nova Lei Federal de Proteção de Dados de 2020 (Suíça), a Lei de Proteção de Dados do Reino Unido de 2018 (DPA 2018) e o Regulamento Geral de Proteção de Dados do Reino Unido (RGPD do Reino Unido), bem como quaisquer leis ou regulamentos estaduais ou federais dos EUA relativos à recolha, utilização, divulgação, segurança ou proteção de dados pessoais, ou à notificação de violações de segurança, designadamente, a Lei de Privacidade do Consumidor da Califórnia de 2018 ("CCPA"), conforme alterada pela Lei dos Direitos de Privacidade da Califórnia de 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:

“EEA+”, para efeitos dos presentes Termos de Privacidade de Dados, significa o Espaço Económico Europeu, composto por quaisquer estados-membros da União Europeia, Islândia, Liechtenstein e Noruega, bem como a Suíça.

“*Incidente de Segurança de Informação*” significa uma violação de segurança da Accenture que conduza à destruição, perda, alteração ou aquisição não autorizada, divulgação, utilização indevida ou acesso accidental ou ilegal a Informações Pessoais do Cliente, transmitidas, armazenadas ou de outro modo tratadas pela Accenture. “*País Restrito*” significa um país, um território ou um ou mais setores específicos dentro desse país que não beneficiam de uma decisão de adequação ao abrigo da Lei de Proteção de Dados aplicável ao exportador de dados.

“*Transferência*” significa a divulgação, partilha, transmissão ou de outra forma disponibilização para tratamento de Informações Pessoais do Cliente por um exportador de dados a um importador de dados sediado noutra jurisdição.

“*Adenda do Reino Unido*” significa a Adenda de Transferência Internacional de Dados às Cláusulas Contratuais Tipo da Comissão da UE VERSÃO B1.0, emitida pelo Comissário de Informação ao abrigo da S119A(1) da Lei de Proteção de Dados de 2018, conforme alterada periodicamente.

O Cliente será o responsável pelo tratamento das Informações Pessoais do Cliente, a Accenture será o subcontratante e cada Parte deverá cumprir a legislação aplicável em matéria de privacidade de dados, na medida em que tal se aplique a essa Parte no âmbito das respetivas funções. O Cliente garante à Accenture que detém todos os direitos necessários para fornecer à Accenture as Informações Pessoais do Cliente, para que o tratamento seja realizado no âmbito dos Serviços. O Cliente será responsável por efetuar todas as notificações necessárias e, quando aplicável, por obter todos os consentimentos necessários das pessoas em causa, conforme exigido pelas Leis de Proteção de Dados aplicáveis no que diz respeito ao tratamento das Informações Pessoais do Cliente.

As Partes reconhecem e aceitam o seguinte quanto ao tratamento de quaisquer Informações Pessoais do Cliente ao abrigo dos presentes Termos de Privacidade de Dados:

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.

1.- Salvo disposição em contrário prevista legalmente, a Accenture tratará as Informações Pessoais do Cliente em nome deste da seguinte forma:

- **O objeto do tratamento** limita-se às Informações Pessoais do Cliente identificadas no presente documento.
- **A natureza e a finalidade do tratamento** consistem na prestação dos Serviços, tal como definidos na descrição dos Serviços na Ordem de Serviço ou no Formulário de Encomenda relevante estabelecidos entre o Cliente e a Accenture.
- **A duração do tratamento** corresponde ao Prazo da Ordem de Serviço ou do Formulário de Encomenda relacionados.
- **Os tipos de Informações Pessoais do Cliente** são: nome, números de telefone, endereço de e-mail, fuso horário, dados de morada, dados de acesso, utilização e autorização do sistema, nome da empresa, dados contratuais (por exemplo, contrato de trabalho, prestadores de serviços) e outros dados contidos no sistema de registos do Cliente.

O Cliente reconhece que os seguintes tipos de Informações Pessoais não podem ser introduzidos pelos Utilizadores Autorizados nos Serviços SaaS nem tratados pela Accenture durante a execução dos Serviços: Número do cartão de débito; Número do cartão de crédito; Relatórios de crédito, pontuações de crédito e alertas de fraude; Saldos de empréstimos ou depósitos; Histórico de pagamentos ou compras (incluindo informações relevantes para o marketing direcionado, por exemplo, histórico de encomendas de produtos, histórico de subscrições de serviços, lista descritiva de consumidores); Informações sobre cuidados médicos, como internamentos, altas, doações de órgãos, medicação e dados relativos ao estado de saúde do titular dos dados; isto abrange as Informações de Saúde Protegidas, conforme definidas no artigo 45 CFR 160.103 da Lei de Portabilidade e Responsabilidade dos Seguros de Saúde dos EUA de 1996 (HIPAA); Informação genética; Identificadores biométricos (ADN, reconhecimento de impressões digitais, da íris ou da retina, reconhecimento facial, geometria da mão, orelha, assinatura e impressões vocais/tecnologia de reconhecimento de voz, verificação ou autenticação de voz); Informações de geolocalização (dados de GPS, movimento, GSP, Wi-Fi e Bluetooth); Dados de "caixa negra"; por exemplo, monitorização telemétrica, a bordo de veículos ou em casa; Conversas (gravações de voz, transcrições ou conversas

ouvidas casualmente); Opiniões políticas (filiação ou apoio a um partido político ou ideologia); Acusações e condenações criminais e registos judiciais.

- **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

- **As categorias de titulares de dados**, salvo disposição em contrário na Ordem de Serviço ou no Formulário de Encomenda aplicável, incluem colaboradores, contratados, parceiros comerciais ou outras pessoas cujas Informações Pessoais se encontrem armazenadas nos Serviços SaaS ou no sistema de registos do Cliente.

- 2.- A Accenture tratará as Informações Pessoais do Cliente apenas em conformidade com as instruções documentadas do Cliente. Os presentes Termos de Privacidade de Dados e a Ordem de Serviço ou o Formulário de Encomenda aplicáveis às Ferramentas de HCM e ERP na Nuvem da Accenture constituem essas instruções iniciais documentadas. A Accenture promoverá todos os esforços razoáveis para seguir quaisquer outras instruções do Cliente, desde que estas sejam exigidas por lei, sejam tecnicamente viáveis e não exijam alterações aos Serviços. Se o Cliente exigir que a Accenture siga uma instrução de tratamento que possa implicar custos adicionais para a Accenture, deverá ser previamente acordada uma alteração à Ordem de Serviço, ao Formulário de Encomenda ou aos Termos e Condições Gerais.

Se o Cliente exigir que a Accenture siga uma instrução de tratamento, apesar de a Accenture ter alertado que tal instrução pode, na opinião da Accenture, infringir uma Lei de Proteção de Dados aplicável, o Cliente assumirá todas as responsabilidades e deverá defender, indemnizar e exonerar a Accenture de qualquer responsabilidade perante todas as reclamações e danos decorrentes de qualquer tratamento continuado em conformidade com essa instrução.

- 3.- A Accenture: (i) não deverá reter, utilizar, divulgar nem tratar de qualquer outra forma as Informações Pessoais do Cliente para qualquer finalidade, incluindo qualquer finalidade comercial, salvo nos termos previstos na Secção 2; (ii) não deverá "vender" nem "partilhar" (conforme cada termo é definido na CCPA, na TDPSA ou noutras leis de privacidade de dados dos EUA, conforme aplicável) as Informações Pessoais do Cliente; (iii) não deverá tratar as Informações Pessoais do Cliente fora do âmbito da relação direta entre a Accenture e o Cliente, salvo se exigido de outra forma por lei;

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

(iv) deverá proporcionar o mesmo nível de proteção exigido pelas obrigações relevantes ao abrigo das leis de privacidade de dados aplicáveis relativamente a tais Informações Pessoais do Cliente recebidas pela Accenture; (v) não deverá combinar as Informações Pessoais do Cliente com quaisquer outros dados pessoais ou informações pessoais que a Accenture receba de, ou em nome de, outra pessoa, ou que recolha a partir das suas próprias interações com pessoas, exceto no âmbito da prestação dos Serviços; (vi) deverá notificar o Cliente em caso de violação ou caso já não consiga cumprir as suas obrigações ao abrigo das Leis de Privacidade de Dados aplicáveis e colaborar com o Cliente para tomar as medidas adequadas para proteger as Informações Pessoais do Cliente; (vii) não deverá tentar desanonimizar, reidentificar ou desagregar quaisquer Informações Pessoais do Cliente anonimizadas, pseudonimizadas ou agregadas. O Cliente aceita que a assinatura destes Termos de Privacidade de Dados pela Accenture se considere que constitui qualquer certificação exigida, nos termos das Leis de Proteção de Dados aplicáveis, para as restrições à venda, retenção, utilização ou divulgação de Dados Pessoais do Cliente aqui abrangidos.

- 4.- Todo o pessoal da Accenture, incluindo subcontratados, autorizados a tratar as Informações Pessoais do Cliente, estarão sujeitos a obrigações de confidencialidade e/ou sujeitos a uma obrigação legal de confidencialidade.
- 5.- Cada Parte deverá implementar medidas de segurança técnicas e organizacionais adequadas para proteger as Informações Pessoais do Cliente contra o tratamento não autorizado ou a perda ou danos acidentais nos respetivos ambientes (por exemplo, sistemas, redes, instalações), e essas normas regerão e controlarão os respetivos ambientes. A Accenture deverá implementar as medidas descritas em pormenor nas proteções de dados dos clientes da Accenture, disponíveis aqui: <https://www.accenture.com/client-data-safeguards>, que foram concebidas para garantir um nível de segurança adequado ao risco associado ao tratamento das Informações Pessoais do Cliente. O Cliente irá ativar a Autenticação Multifator nos seus sistemas de SuccessFactors. Além de prestar os Serviços a partir das instalações da Accenture, o pessoal da Accenture poderá prestar os Serviços ou qualquer parte dos mesmos à distância, desde que essa prestação à distância não (i) afete negativamente a capacidade da

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.

Accenture de cumprir as suas obrigações nos termos da Ordem de Serviço ou do Formulário de Encomenda relevante; nem (ii) implique qualquer aumento dos Honorários aplicáveis.

Para Serviços prestados à distância, quaisquer exigências contratuais de realizar controlos de segurança físicos e ambientais (por ex., baías seguras; vigilantes; CCTV) nos locais de serviço da Accenture não se aplicarão a locais de trabalho à distância. Além disso, quando pessoal da Accenture tiver de aceder a sistemas do Cliente a partir de um local de trabalho à distância, esse acesso ocorrerá apenas usando dispositivos da Accenture.

6.- O Cliente autoriza, de um modo geral, a contratação das afiliadas da Accenture, do Fornecedor da Nuvem da Accenture e dos outros terceiros indicados na Ordem de Serviço ou no Formulário de Encomenda aplicável, na qualidade de subcontratantes ulteriores. A Accenture exigirá contratualmente (incluindo através de cláusulas contratuais-tipo, contratos de subcontratação ulterior ou, no que diz respeito às afiliadas da Accenture, contratos intraempresas, conforme aplicável) que quaisquer subcontratantes ulteriores cumpram obrigações de proteção de dados equivalentes às que a Accenture é obrigada a cumprir nos termos do presente contrato, na medida em que sejam aplicáveis aos serviços subcontratados dos subcontratantes ulteriores. Quando aplicável, quaisquer Transferências de Informações Pessoais do Cliente para subcontratantes ulteriores externos ("Subcontratantes Ulteriores Externos") serão geridas pela Accenture em conformidade com a legislação aplicável em matéria de privacidade de dados, nomeadamente através da utilização de mecanismos de transferência de dados celebrados pela Accenture com os Subcontratantes Ulteriores Externos relevantes a nível global. A Accenture continuará a ser inteiramente responsável pelo desempenho dos subcontratantes ulteriores, de acordo com o disposto no contrato celebrado com o Cliente. A Accenture deverá notificar o Cliente por correio eletrónico de todas as alterações quanto aos subcontratantes ulteriores autorizados, e o Cliente deverá de imediato, e em qualquer caso no prazo de 10 dias úteis, notificar a Accenture por escrito de qualquer oposição razoável a essas alterações. Caso o Cliente suscite qualquer oposição, as Partes deverão discutir e resolver qualquer desacordo através do procedimento de resolução de litígios indicado nos TCG. Caso não seja possível chegar a uma resolução,

- o Cliente só terá o direito de resolver a Ordem de Serviço ou o Formulário de Encomenda em causa mediante notificação por escrito à Accenture, desde que o Cliente envie essa notificação no prazo de noventa (90) dias a contar do termo do período de resolução de litígios indicado nos TCG.
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.
- 7.- Tendo em conta a natureza dos Serviços e a informação de que a Accenture dispõe, a Accenture deverá cooperar com o Cliente, na medida do razoavelmente solicitado, para o apoiar no cumprimento das suas obrigações ao abrigo das Leis de Privacidade de Dados no que diz respeito a: (i) implementação, por parte do Cliente, de medidas de segurança adequadas; (ii) obrigação do Cliente de responder aos pedidos dos titulares de dados do Cliente; (iii) obrigação do Cliente de notificar as autoridades reguladoras e os titulares dos dados sobre uma violação de dados pessoais relativa às Informações Pessoais do Cliente, conforme exigido pelas Leis de Privacidade de Dados aplicáveis; (iv) obrigação do Cliente de realizar avaliações de impacto em matéria de proteção de dados; e (v) obrigação do Cliente de consultar as autoridades reguladoras quando tal for exigido pelas Leis de Privacidade de Dados aplicáveis.
- 8.- A Accenture deverá manter procedimentos para detetar e responder a Incidentes de Segurança de Informação. Se ocorrer um Incidente de Segurança de Informação que, em termos razoáveis, possa comprometer a segurança ou a privacidade de Informações Pessoais do Cliente, a Accenture notificará de imediato o Cliente, sem atrasos injustificados. A Accenture colaborará com o Cliente na investigação do Incidente de Segurança de Informação e, tendo em conta a natureza dos Serviços prestados e as informações à disposição da Accenture, prestará assistência ao Cliente, segundo o que razoavelmente for solicitado, em relação às obrigações de notificação de violação do Cliente ao abrigo de quaisquer Leis de Privacidade de Dados.
- 9.- Após o termo ou a resolução da Ordem de Serviço ou do Formulário de Encomenda aplicável, a Accenture **deverá devolver ou destruir** quaisquer Informações Pessoais do Cliente, de acordo com as instruções do Cliente. Para maior clareza, as Informações Pessoais do Cliente armazenadas nos suportes de cópias de segurança de TI partilhados pela Accenture serão apagadas no prazo de noventa (90) dias, em conformidade com a política interna da Accenture.

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

10.-A Accenture disponibilizará ao Cliente as informações que este solicitar de forma razoável para comprovar o cumprimento, por parte da Accenture, das suas obrigações previstas nos presentes Termos de Privacidade de Dados, e a Accenture submeter-se-á a auditorias e inspeções realizadas pelo Cliente (ou por terceiros designados pelo Cliente), de acordo com um processo a acordar mutuamente, de forma a evitar a interrupção dos Serviços e a proteger as informações confidenciais da Accenture, dos seus subcontratantes ulteriores autorizados e dos seus outros clientes, e de acordo com os seguintes princípios:

- auditoria limitada a uma vez por ano;
- não ultrapassar 3 dias úteis, salvo acordo em contrário por escrito entre as partes.
- notificação por escrito com antecedência razoável (pelo menos 60 dias, a menos que uma autoridade de proteção de dados exija que o Cliente assuma o controlo mais cedo, ao abrigo de Leis de Privacidade de Dados imperativas).
- o âmbito e a agenda da auditoria devem ser determinados antecipadamente.

No que se refere a esta cláusula, a Accenture deverá informar o Cliente se, na opinião da Accenture, alguma instrução do Cliente infringir a Lei de Proteção de Dados aplicável.

No contexto dos Serviços SaaS, o Cliente reconhece que os Subcontratantes Ulteriores Externos da Accenture, como o Fornecedor da Nuvem, recorrem a auditores externos e independentes para auditar e verificar a adequação das suas medidas de segurança, incluindo a segurança dos seus centros de dados físicos, e elaboram um relatório de auditoria, disponibilizado anualmente ("Relatório"). Os Relatórios podem ser considerados Informação Confidencial dos Subcontratantes Ulteriores Externos e serão disponibilizados ao Cliente, a pedido deste, desde que o Cliente assine o acordo de confidencialidade tipo do Subcontratante Ulterior Externo, quando aplicável. O Cliente aceita exercer qualquer direito de realizar uma auditoria ou inspeção do Subcontratante Ulterior Externo, nomeadamente ao abrigo de qualquer mecanismo de transferência aplicável, dando instruções à Accenture para obter o Relatório do Subcontratante Ulterior Externo em questão, tal como se descreve nesta cláusula. O Cliente pode alterar esta instrução a

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

qualquer momento, mediante notificação por escrito dirigida à Accenture, desde que, caso o Subcontratante Ulterior Externo se recuse a submeter-se a uma auditoria ou inspeção solicitada pelo Cliente, a Accenture não venha a estar em incumprimento dos presentes Termos de Privacidade de Dados, embora o Cliente tenha o direito de resolver a Ordem de Serviço a que tal pedido se refere, mediante notificação, com antecedência de 30 dias, dirigida à Accenture. Nenhuma disposição da presente cláusula deve ser interpretada no sentido de afetar os direitos de qualquer autoridade de controlo ou do titular dos dados ao abrigo das Leis de Proteção de Dados aplicáveis.

11.-O Cliente reconhece e aceita que, para a prestação dos Serviços, as Informações Pessoais do Cliente poderão ser transferidas para fora do país de onde essas Informações Pessoais são originárias. Nesse caso, aplicam-se as seguintes disposições:

11.1 Transferências de Informações Pessoais do Cliente a partir de qualquer país do EEE+

(a) Quaisquer Transferências de Informações Pessoais do Cliente de qualquer país do EEE+ para afiliadas da Accenture localizadas num País Restrito serão reguladas pelas BCR de Subcontratante da UE da Accenture, que são integradas por referência no presente documento e constituem parte integrante dos presentes Termos de Privacidade de Dados, bem como da respetiva Ordem de Serviço, do Formulário de Encomenda e dos TCG.

(b) Responsabilidades das partes.

(i) **Accenture como exportador de dados.** Se a entidade contratante da Accenture estiver sediada no EEE+, as Partes reconhecem e aceitam que a Accenture será considerada a exportadora de dados, e as afiliadas relevantes da Accenture serão consideradas as importadoras de dados. A Accenture será responsável por realizar qualquer avaliação de impacto de transferência necessária.

(ii) **Cliente como exportador de dados.** Se a entidade contratante da Accenture estiver sediada fora do EEE+, as Partes reconhecem e aceitam que (1) o Cliente e/ou as suas agrupadas relevantes serão considerados o(s) exportador(es) de dados e cumprirão as obrigações correspondentes ao abrigo do RGPD/da Lei de Proteção de Dados da Suíça, incluindo a realização de qualquer avaliação de impacto de transferência necessária, e (2) a Accenture/as afiliadas da Accenture relevantes será(ão)

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

considerada(s) importador(es) de dados e cumprirá(ão) as obrigações correspondentes ao abrigo do RGPD/da Lei de Proteção de Dados da Suíça, incluindo a cooperação com o(s) exportador(es) de dados na avaliação dos riscos das Transferências, disponibilizando uma avaliação do risco de transferência do país para os Países Restritos relevantes.

(c) Em qualquer caso, o Cliente é responsável e compromete-se a: (i) informar os titulares de dados em causa sobre as transferências e as BCR de Subcontratante da UE da Accenture, que podem ser disponibilizadas aos titulares de dados mediante pedido, juntamente com uma cópia dos presentes Termos de Privacidade de Dados, após a supressão de qualquer informação comercial sensível e confidencial; e (ii) informar especificamente os titulares dos dados dos Países Restritos de destino, se as Transferências envolverem categorias especiais de dados pessoais.

(d) Se o Cliente atuar como subcontratante no que respeita às Informações Pessoais do Cliente sujeitos à Transferência, o Cliente declara e garante que as instruções de tratamento do Cliente, incluindo no que respeita às Transferências de qualquer país EEA+, foram autorizadas pelo(s) responsável(is) pelo tratamento de dados aplicável(eis). Nesse caso, o Cliente deverá aplicar as BCR de Subcontratante da UE da Accenture em nome ou para benefício do(s) responsável(is) pelo tratamento real(ais) das Informação Pessoais do Cliente, em conformidade com os presentes Termos de Privacidade de Dados e com a respetiva Ordem de Serviço, Formulário de Encomenda e os TCG.

(e) As Partes acordam ainda que quaisquer referências aos "Contratos de Serviço ao Cliente" feitas nas BCR de Subcontratante da UE da Accenture, serão consideradas como feitas à respetiva Ordem de Serviço, ao Formulário de Encomenda e aos TCG. De acordo com a respetiva Ordem de Serviço, o Formulário de Encomenda e os TCG, o Cliente terá o direito de fazer valer as BCR de Subcontratante da UE da Accenture contra o grupo Accenture, incluindo medidas judiciais e o direito a receber uma indemnização.

11.2 Transferências de Informações Pessoais do Clientes a partir do Reino Unido. Quaisquer Transferências de Informações Pessoais do Cliente do Reino Unido para uma Afiliada da Accenture localizada num País Restrito serão reguladas pela Adenda do Reino Unido. Se a entidade contratante da Accenture estiver sediada no Reino Unido, quaisquer

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

Transferências de Informações Pessoais do Cliente do Reino Unido para uma agrupada da Accenture localizada num País Restrito serão reguladas pela Adenda do Reino Unido que integra o Módulo Três – Subcontratante para Subcontratante das Cláusulas Contratuais Tipo da UE entre a Accenture e a(s) agrupada(s) aplicável(eis) da Accenture. Se a entidade contratante da Accenture estiver sediada fora do Reino Unido, o Cliente/agrupadas do Cliente que atuem como exportador(es) de dados e a Accenture/afiliada(s) da Accenture aplicável(eis), que atuem como importadores(es) de dados, deverão executar a Adenda do Reino Unido integrando o módulo apropriado das Cláusulas Contratuais Tipo da UE com base nas Transferências ocorridas ao abrigo da Ordem de Serviço ou do Formulário de Encomenda aplicável.

11.3 Transferências de Informações Pessoais do Cliente a partir de países fora do EEE+ e do Reino Unido. Sem prejuízo do disposto na Cláusula 11.1 supra, mediante indicação do Cliente, as BCR de Subcontratante da UE da Accenture regerão quaisquer Transferências de Informações Pessoais do Cliente efetuadas pelo Cliente e/ou por uma afiliada do Cliente a partir de qualquer país fora do EEE+ e do Reino Unido para afiliadas da Accenture localizadas em Países Restritos, conforme detalhado na Ordem de Serviço ou no Formulário de Encomenda relevante. Caso seja necessário um mecanismo de transferência diferente, nos termos das Leis de Proteção de Dados aplicáveis à entidade do Cliente em causa que atua como exportador de dados, as Partes colaborarão de forma célere e de boa-fé para estabelecer o mecanismo de transferência adequado a implementar.

11.4 Mecanismo de Transferência. No caso de os mecanismos de transferência aqui acordados pelas Partes serem alterados, substituídos ou deixarem de ser autorizados como um meio para fornecer "proteção adequada" em relação às Transferências de Informações Pessoais do Cliente, as Partes trabalharão em conjunto de forma diligente e de boa-fé para estabelecer outro mecanismo de transferência válido e/ou implementar medidas complementares, conforme o que for necessário para criar proteções adequadas para essas Informações Pessoais do Cliente.

11.5 Leis de Proteção de Dados. Quaisquer acordos de transferência de dados (incluindo, entre outros, quaisquer Cláusulas Contratuais Tipo) que as partes ou as suas afiliadas possam celebrar no âmbito dos Serviços prestados nos termos de uma Ordem de Serviço ou de um Formulário de Encomenda e dos TCG, serão considerados parte

prejudice to the rights of any data subjects under any data transfer agreement, governed by the terms thereof.

integrante da respetiva Ordem de Serviço, do Formulário de Encomenda e dos TCG e, sem prejuízo dos direitos de quaisquer titulares de dados ao abrigo de qualquer acordo de transferência de dados, regulados pelos termos dos mesmos.