

PERSONAL DATA PROCESSING AGREEMENT FOR SAP CLOUD SERVICES

ACORDO DE TRATAMENTO DE DADOS PESSOAIS PARA SERVIÇOS SAP CLOUD

1. BACKGROUND

1.1 Purpose and Application. This document (“DPA”) is incorporated into the Agreement and forms part of a written (including in electronic form) contract between SAP and Customer. This DPA applies to Personal Data processed by SAP and its Subprocessors in connection with its provision of the Cloud Service. This DPA does not apply to non-production environments of the Cloud Service if such environments are made available by SAP, and Customer shall not store Personal Data in such environments.

1.2 Structure. Appendices 1 and 2 are incorporated into and form part of this DPA. They set out the agreed subject-matter, the nature and purpose of the processing, the type of Personal Data, categories of data subjects and the applicable technical and organizational measures.

1.3 GDPR. SAP and Customer agree that it is each party’s responsibility to review and adopt requirements imposed on Controllers and Processors by the General Data Protection Regulation 2016/679 (“GDPR”), in particular with regards to Articles 28 and 32 to 36 of the GDPR, if and to the extent applicable to Personal Data of Customer/Controllers that is processed under the DPA. For illustration purposes, Appendix 3 lists the relevant GDPR requirements and the corresponding sections in this DPA.

1.4 Governance. SAP acts as a Processor and Customer and those entities that it permits to use the Cloud Service act as Controllers under the DPA. Customer acts as a single point of contact and is solely responsible for obtaining any relevant authorizations, consents and permissions for the processing of Personal Data in accordance with this DPA, including, where applicable approval by Controllers to use SAP as a Processor. Where authorizations, consent, instructions or permissions are provided by Customer these are provided not only on behalf of the Customer but also on behalf of any other Controller using the Cloud Service. Where SAP informs or gives notice to Customer, such information or notice is deemed received by those Controllers permitted by Customer to use the Cloud Service and it is Customer’s responsibility to forward such information and notices to the relevant Controllers.

1. CONTEXTO

1.1 Finalidade e Aplicação. Este documento (“ATD”) está incorporado no Contrato e constitui parte de um contrato por escrito (que inclui a forma eletrónica), celebrado entre a SAP e o Cliente. Este ATD é aplicável aos Dados Pessoais tratados pela SAP e respetivos Subcontratantes Ulteriores, em conjugação com a disponibilização do Serviço Cloud. Este ATD não se aplica a ambientes não produtivos do Serviço Cloud, caso tais ambientes sejam disponibilizados pela SAP, não podendo o Cliente armazenar Dados Pessoais em tais ambientes.

1.2 Estrutura. Os Apêndices 1 e 2 estão incorporados no presente ATD, constituindo parte integrante do mesmo. Eles estabelecem a matéria acordada, a natureza e a finalidade do tratamento, o tipo de Dados Pessoais, as categorias de titulares dos dados e as medidas técnicas e organizacionais aplicáveis.

1.3 RGPD. A SAP e o Cliente aceitam que é da responsabilidade de cada uma das partes analisar e adotar os requisitos impostos aos Responsáveis pelo Tratamento de Dados e Subcontratantes pelo Regulamento Geral de Proteção de Dados 2016/679 (“RGPD”), em particular no que se refere aos Artigos 28º e 32º a 36º do RGPD, se e na medida do aplicável aos Dados Pessoais do Cliente/Responsáveis pelo Tratamento de Dados, tratados ao abrigo do ATD. Para efeitos de ilustração, o Apêndice 3 enumera os requisitos relevantes do RGPD e as secções correspondentes no presente ATD.

1.4 Regulamentação. A SAP atua na qualidade de Subcontratante e o Cliente e as entidades autorizadas a utilizar o Serviço Cloud atuam como Responsáveis pelo Tratamento de Dados, nos termos do presente ATD. O Cliente atua como único ponto de contacto, sendo o responsável exclusivo por obter todos os consentimentos, autorizações e permissões relevantes para o tratamento de Dados Pessoais, de acordo com o presente ATD, incluindo, quando aplicável, a aprovação dos Responsáveis pelo Tratamento de Dados para utilizar a SAP como Subcontratante. Quando o Cliente disponibilizar autorizações, consentimentos, instruções ou permissões, não o faz exclusivamente em seu nome, mas também em nome de qualquer outro Responsável pelo Tratamento de Dados que utilize o Serviço Cloud. Quando a SAP disponibilizar informações ou avisos ao Cliente, tais informações ou avisos são considerados recebidos pelos Responsáveis pelo Tratamento de Dados autorizados pelo Cliente a utilizar o Serviço Cloud, sendo da responsabilidade do Cliente encaminhar tais informações e avisos

aos Responsáveis pelo Tratamento de Dados relevantes.

2. SECURITY OF PROCESSING

2.1 Appropriate Technical and Organizational Measures. SAP has implemented and will apply the technical and organizational measures set forth in [Appendix 2](#). Customer has reviewed such measures and agrees that as to the Cloud Service selected by Customer in the Order Form the measures are appropriate taking into account the state of the art, the costs of implementation, nature, scope, context and purposes of the processing of Personal Data.

2.2 Changes. SAP applies the technical and organizational measures set forth in Appendix 2 to SAP's entire customer base hosted out of the same Data Center and receiving the same Cloud Service. SAP may change the measures set out in Appendix 2 at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

3. SAP OBLIGATIONS

3.1 Instructions from Customer. SAP will process Personal Data only in accordance with documented instructions from Customer. The Agreement (including this DPA) constitutes such documented initial instructions and each use of the Cloud Service then constitutes further instructions. SAP will use reasonable efforts to follow any other Customer instructions, as long as they are required by Data Protection Law, technically feasible and do not require changes to the Cloud Service. If any of the before-mentioned exceptions apply, or SAP otherwise cannot comply with an instruction or is of the opinion that an instruction infringes Data Protection Law, SAP will immediately notify Customer (email permitted).

3.2 Processing on Legal Requirement. SAP may also process Personal Data where required to do so by applicable law. In such a case, SAP shall inform Customer of that legal requirement before processing unless that law prohibits such information on important grounds of public interest.

3.3 Personnel. To process Personal Data, SAP and its Subprocessors shall only grant access to authorized personnel who have committed themselves to confidentiality. SAP and its Subprocessors will regularly train personnel having access to Personal Data in applicable data security and data privacy measures.

2. SEGURANÇA DO TRATAMENTO

2.1 Medidas Técnicas e Organizacionais Adequadas. A SAP implementou e aplicará as medidas técnicas e organizacionais definidas no [Apêndice 2](#). O Cliente analisou essas medidas e aceita que, no que se refere ao Serviço Cloud selecionado pelo Cliente no Formulário de Encomenda, as medidas são adequadas, tendo em consideração o estado da tecnologia, os custos de implementação, a natureza, o âmbito, o contexto e as finalidades do tratamento de Dados Pessoais.

2.2 Alterações. A SAP aplica as medidas técnicas e organizacionais definidas no Apêndice 2 à totalidade da base de clientes da SAP, alojada no mesmo Centro de Tratamento de Dados e que recebe o mesmo Serviço Cloud. A SAP poderá alterar as medidas definidas no Apêndice 2 em qualquer momento sem aviso prévio, desde que mantenha um nível de segurança equivalente ou superior. Medidas individuais poderão ser substituídas por novas medidas que sirvam o mesmo propósito sem diminuir o nível de segurança que protege os Dados Pessoais.

3. OBRIGAÇÕES DA SAP

3.1 Instruções do Cliente. A SAP tratará os Dados Pessoais exclusivamente de acordo com as instruções documentadas do Cliente. O Contrato (incluindo o presente ATD) constitui essas instruções iniciais documentadas e cada utilização do Serviço Cloud configura mais instruções. A SAP envidará todos os esforços, na medida do razoável, para seguir quaisquer outras instruções do Cliente, desde que tais instruções sejam exigidas pela Legislação sobre Proteção de Dados, tecnicamente viáveis e não requeiram alterações ao Serviço Cloud. Caso qualquer uma das exceções acima mencionadas seja aplicável, ou a SAP não possa cumprir, de outro modo, uma instrução ou considere que uma instrução viola a Legislação sobre Proteção de Dados, a SAP notificará, de imediato, o Cliente (e-mail permitido).

3.2 Tratamento por Requisito Legal. A SAP poderá igualmente tratar Dados Pessoais quando tal lhe seja exigido pela legislação aplicável. Nesse caso, a SAP informará o Cliente sobre tal requisito legal antes do tratamento, salvo se a legislação proibir tal informação, com base em fundamentos importantes de interesse público.

3.3 Pessoal. Para o tratamento de Dados Pessoais, a SAP e respetivos Subcontratantes Ulteriores apenas concederão acesso a pessoal autorizado que se tenha comprometido a manter a confidencialidade. A SAP e respetivos Subcontratantes Ulteriores darão regularmente formação a pessoal com acesso aos Dados

3.4 Cooperation. At Customer's request, SAP will reasonably cooperate with Customer and Controllers in dealing with requests from Data Subjects or regulatory authorities regarding SAP's processing of Personal Data or any Personal Data Breach. SAP shall notify the Customer as soon as reasonably practical about any request it has received from a Data Subject in relation to the Personal Data processing, without itself responding to such request without Customer's further instructions, if applicable. SAP shall provide functionality that supports Customer's ability to correct or remove Personal Data from the Cloud Service, or restrict its processing in line with Data Protection Law. Where such functionality is not provided, SAP will correct or remove any Personal Data, or restrict its processing, in accordance with the Customer's instruction and Data Protection Law.

3.5 Personal Data Breach Notification. SAP will notify Customer without undue delay after becoming aware of any Personal Data Breach and provide reasonable information in its possession to assist Customer to meet Customer's obligations to report a Personal Data Breach as required under Data Protection Law. SAP may provide such information in phases as it becomes available. Such notification shall not be interpreted or construed as an admission of fault or liability by SAP.

3.6 Data Protection Impact Assessment. If, pursuant to Data Protection Law, Customer (or its Controllers) are required to perform a data protection impact assessment or prior consultation with a regulator, at Customer's request, SAP will provide such documents as are generally available for the Cloud Service (for example, this DPA, the Agreement, audit reports or certifications). Any additional assistance shall be mutually agreed between the Parties.

4. DATA EXPORT AND DELETION

4.1 Export and Retrieval by Customer. During the Subscription Term and subject to the Agreement, Customer can access its Personal Data at any time. Customer may export and retrieve its Personal Data in a standard format. Export and retrieval may be subject to technical limitations, in which case SAP and Customer

Pessoais sobre medidas aplicáveis de segurança e privacidade de dados.

3.4 Cooperação. Mediante pedido do Cliente, a SAP apoiará, na medida do razoável, o Cliente e Responsáveis pelo Tratamento de Dados a lidar com pedidos de Titulares dos Dados ou de autoridades reguladoras, relativos ao tratamento de Dados Pessoais por parte da SAP ou a qualquer Violação dos Dados Pessoais. A SAP notificará o Cliente, logo que viável na medida do razoável, sobre qualquer solicitação que tenha recebido de um Titular dos Dados, relativamente ao tratamento dos Dados Pessoais, antes de responder a tal solicitação sem receber instruções do Cliente, caso tal seja aplicável. A SAP disponibilizará funcionalidades que suportem a capacidade do Cliente para corrigir ou remover Dados Pessoais do Serviço Cloud, ou restringir o seu tratamento, de acordo com a Legislação sobre Proteção de Dados. Quando tais funcionalidades não sejam disponibilizadas, a SAP corrigirá ou removerá quaisquer Dados Pessoais, ou restringirá o respetivo tratamento, de acordo com a instrução do Cliente e a Legislação sobre Proteção de Dados.

3.5 Notificação de Violação de Dados Pessoais. A SAP notificará o Cliente, de imediato, depois de tomar conhecimento sobre qualquer Violação de Dados Pessoais e fornecerá, na medida do razoável, as informações que estejam na sua posse, para ajudar o Cliente a cumprir as respetivas obrigações de notificação de uma Violação de Dados Pessoais, nos termos da Legislação sobre proteção de Dados. A SAP poderá disponibilizar tais informações de modo faseado, à medida que se tornem disponíveis. Tal notificação não será interpretada nem considerada como uma admissão de culpa ou de responsabilidade por parte da SAP.

3.6 Avaliação do Impacto da Proteção de Dados. Caso, nos termos da Legislação sobre Proteção de Dados, seja exigida ao Cliente (ou respetivos Responsáveis pelo Tratamento de Dados) a realização de uma avaliação do impacto da proteção de dados ou a consulta prévia de um regulador, a SAP, mediante pedido do Cliente, disponibilizará todos os documentos disponíveis de modo geral, relativos ao Serviço Cloud (por exemplo, o presente ATD, o Contrato, relatórios de auditoria ou certificações). Qualquer assistência adicional será acordada mutuamente entre as Partes.

4. EXPORTAÇÃO E ELIMINAÇÃO DE DADOS

4.1 Exportação e Recuperação por parte do Cliente. Durante o Período de Subscrição, e sujeito ao Contrato, o Cliente pode aceder em qualquer momento aos respetivos Dados Pessoais. O Cliente poderá exportar e recuperar os seus Dados Pessoais num formato padrão. A exportação e recuperação poderão estar sujeitas a limitações técnicas, caso em que a

will find a reasonable method to allow Customer access to Personal Data.

4.2 Deletion. Before the Subscription Term expires, Customer may use SAP's self-service export tools (as available) to perform a final export of Personal Data from the Cloud Service (which shall constitute a "return" of Personal Data). At the end of the Subscription Term, Customer hereby instructs SAP to delete the Personal Data remaining on servers hosting the Cloud Service within a reasonable time period in line with Data Protection Law (not to exceed six months) unless applicable law requires retention.

5. CERTIFICATIONS AND AUDITS

5.1 Customer Audit. Customer or its independent third party auditor reasonably acceptable to SAP (which shall not include any third party auditors who are either a competitor of SAP or not suitably qualified or independent) may audit SAP's control environment and security practices relevant to Personal Data processed by SAP only if:

- (a) SAP has not provided sufficient evidence of its compliance with the technical and organizational measures that protect the production systems of the Cloud Service through providing either: (i) a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate); or (ii) a valid ISAE3402 and/or ISAE3000 or other SOC1-3 attestation report. Upon Customer's request audit reports or ISO certifications are available through the third party auditor or SAP;
- (b) A Personal Data Breach has occurred;
- (c) An audit is formally requested by Customer's data protection authority; or
- (d) Mandatory Data Protection Law provides Customer with a direct audit right and provided that Customer shall only audit once in any twelve month period unless mandatory Data Protection Law requires more frequent audits.

5.2 Other Controller Audit. Any other Controller may audit SAP's control environment and security practices relevant to Personal Data processed by SAP in line with Section 5.1 only if any of the cases set out in Section 5.1 applies to such other Controller. Such audit must be undertaken through and by Customer as set out in Section 5.1 unless the audit must be

SAP e o Cliente encontrarão um método razoável que permita ao Cliente aceder aos Dados Pessoais.

4.2 Eliminação. Antes de o Período de Subscrição caducar, o Cliente poderá utilizar as ferramentas de exportação self-service da SAP (quando disponíveis) para realizar uma exportação final dos Dados Pessoais a partir do Serviço Cloud (o que constituirá uma "devolução" de Dados Pessoais"). No final do Período de Subscrição, o Cliente instruirá a SAP no sentido de eliminar os Dados Pessoais que permaneçam nos servidores que alojam o Serviço Cloud, dentro de um prazo razoável de acordo com a Legislação sobre Proteção de Dados (que não excederá os seis meses), salvo se a legislação aplicável exigir a retenção.

5. CERTIFICAÇÕES E AUDITORIAS

5.1 Auditoria do Cliente. O Cliente, ou o respetivo auditor externo independente razoavelmente aceite pela SAP (que não incluirá quaisquer auditores externos que sejam concorrentes da SAP ou que não sejam adequadamente qualificados ou independentes), poderá auditar o ambiente de controlo e as práticas de segurança da SAP, relevantes para os Dados Pessoais tratados pela SAP, exclusivamente se:

- (a) A SAP não tiver comprovado, em medida suficiente, o respetivo cumprimento das medidas técnicas e organizacionais que protegem os sistemas produtivos do Serviço Cloud, disponibilizando: (i) uma certificação relativa ao cumprimento da ISO 27001 ou de outras normas (âmbito definido no certificado); ou (ii) um relatório de certificação ISAE3402 e/ou ISAE3000, ou outro relatório de certificação SOC1-3, válidos. Mediante pedido do Cliente, os relatórios de auditoria ou as certificações ISO são disponibilizados pelo auditor externo ou pela SAP;
- (b) Tiver ocorrido uma Violação dos Dados Pessoais;
- (c) Tiver sido formalmente solicitada uma auditoria pela autoridade para proteção de dados do Cliente; ou
- (d) A Legislação obrigatória sobre Proteção de Dados conceder ao Cliente um direito de auditoria direto e desde que o Cliente apenas efetue uma auditoria em cada período de doze meses, salvo se a Legislação obrigatória sobre Proteção de Dados exigir auditorias mais frequentes.

5.2 Auditoria de outro Responsável pelo Tratamento de Dados. Qualquer outro Responsável pelo Tratamento de Dados poderá auditar o ambiente de controlo e as práticas de segurança da SAP, relevantes para os Dados Pessoais tratados pela SAP, de acordo com a Secção 5.1, exclusivamente se qualquer um dos casos estabelecidos na Secção 5.1 for

undertaken by the other Controller itself under Data Protection Law. If several Controllers whose Personal Data is processed by SAP on the basis of the Agreement require an audit, Customer shall use all reasonable means to combine the audits and to avoid multiple audits.

5.3 Scope of Audit. Customer shall provide at least sixty days advance notice of any audit unless mandatory Data Protection Law or a competent data protection authority requires shorter notice. The frequency and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited in time to a maximum of three business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. Customer shall provide the results of any audit to SAP.

5.4 Cost of Audits. Customer shall bear the costs of any audit unless such audit reveals a material breach by SAP of this DPA, then SAP shall bear its own expenses of an audit. If an audit determines that SAP has breached its obligations under the DPA, SAP will promptly remedy the breach at its own cost.

6. SUBPROCESSORS

6.1 Permitted Use. SAP is granted a general authorization to subcontract the processing of Personal Data to Subprocessors, provided that:

- (a)** SAP or SAP SE on its behalf shall engage Subprocessors under a written (including in electronic form) contract consistent with the terms of this DPA in relation to the Subprocessor's processing of Personal Data. SAP shall be liable for any breaches by the Subprocessor in accordance with the terms of this Agreement;
- (b)** SAP will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection to establish that it is capable of providing the level of protection of Personal Data required by this DPA; and

aplicável a esse outro Responsável pelo Tratamento de Dados. Tal auditoria terá de ser realizada pelo Cliente, tal como definido na Secção 5.1, a menos que a auditoria tenha de ser realizada pelo outro Responsável pelo Tratamento de dados, ao abrigo da Legislação sobre Proteção de Dados. Caso vários Responsáveis pelo Tratamento de Dados, cujos Dados Pessoais sejam tratados pela SAP com base no Contrato, requeiram uma auditoria, o Cliente utilizará todos os meios necessários, na medida do razoável, para combinar as auditorias e evitar auditorias múltiplas.

5.3 Âmbito da Auditoria. O Cliente fornecerá um aviso prévio de, pelo menos, sessenta dias, relativamente a qualquer auditoria, salvo se a Legislação obrigatória sobre Proteção de Dados ou qualquer autoridade competente para proteção de dados exigir um aviso mais curto. A frequência e o âmbito de quaisquer auditorias serão acordados mutuamente entre as partes, de modo razoável e em boa-fé. As auditorias do Cliente serão temporalmente limitadas a um máximo de três dias úteis. Além destas restrições, as partes utilizarão certificações atuais ou outros relatórios de auditoria para evitar ou minimizar a existência de auditorias repetidas. O Cliente disponibilizará à SAP os resultados de qualquer auditoria.

5.4 Custo de Auditorias. O Cliente suportará os custos de qualquer auditoria, a menos que tal auditoria revele uma violação grave, por parte da SAP, deste ATD, caso em que a SAP suportará as respetivas despesas em relação a uma auditoria. Caso uma auditoria determine que a SAP violou as suas obrigações nos termos do ATD, a SAP sanará, de imediato, a violação às suas próprias custas.

6. SUBCONTRATANTES ULTERIORES

6.1 Utilização Permitida. É concedida à SAP uma autorização geral para subcontratar o tratamento de Dados Pessoais a Subcontratantes Ulteriores, desde que:

- (a)** A SAP, ou a SAP SE em seu nome, contrate os Subcontratantes Ulteriores ao abrigo de um contrato por escrito (incluindo a forma eletrónica), consistente com os termos do presente ATD, no que se refere ao tratamento dos Dados Pessoais por parte do Subcontratante Ulterior. A SAP assumirá a responsabilidade por quaisquer violações do Subcontratante Ulterior, de acordo com o termos do presente Contrato;
- (b)** A SAP avalie as práticas de segurança, privacidade e de confidencialidade de um Subcontratante Ulterior antes da seleção, de modo a estabelecer que tal entidade tem capacidade para fornecer o nível de proteção dos Dados Pessoais exigido pelo presente ATD; e

- (c) SAP's list of Subprocessors in place on the effective date of the Agreement is published by SAP or SAP will make it available to Customer upon request, including the name, address and role of each Subprocessor SAP uses to provide the Cloud Service.
- 6.2 New Subprocessors.** SAP's use of Subprocessors is at its discretion, provided that:
- (a) SAP will inform Customer in advance (by email or by posting on the support portal available through SAP Support) of any intended additions or replacements to the list of Subprocessors including name, address and role of the new Subprocessor; and
- (b) Customer may object to such changes as set out in Section 6.3.
- 6.3 Objections to New Subprocessors.**
- (a) If Customer has a legitimate reason under Data Protection Law to object to the new Subprocessors' processing of Personal Data, Customer may terminate the Agreement (limited to the Cloud Service for which the new Subprocessor is intended to be used) on written notice to SAP. Such termination shall take effect at the time determined by the Customer which shall be no later than thirty days from the date of SAP's notice to Customer informing Customer of the new Subprocessor. If Customer does not terminate within this thirty day period, Customer is deemed to have accepted the new Subprocessor.
- (b) Within the thirty day period from the date of SAP's notice to Customer informing Customer of the new Subprocessor, Customer may request that the parties come together in good faith to discuss a resolution to the objection. Such discussions shall not extend the period for termination and do not affect SAP's right to use the new Subprocessor(s) after the thirty day period.
- (c) Any termination under this Section 6.3 shall be deemed to be without fault by either party and shall be subject to the terms of the Agreement.
- 6.4 Emergency Replacement.** SAP may replace a Subprocessor without advance notice where the reason for the change is outside of SAP's reasonable control and prompt replacement is required for security or other urgent reasons. In this case, SAP will inform Customer of the replacement Subprocessor as soon as possible
- (c) A lista de Subcontratantes Ulteriores da SAP disponíveis na data de entrada em vigor do Contrato esteja publicada pela SAP ou a SAP a disponibilize ao Cliente, mediante pedido, devendo tal lista incluir o nome, endereço e função de cada Subcontratante Ulterior que a SAP utiliza para prestar o Serviço Cloud.
- 6.2 Novos Subcontratantes Ulteriores.** A utilização de Subcontratantes Ulteriores por parte da SAP é efetuada a título próprio, desde que:
- (a) A SAP informe antecipadamente o Cliente (por e-mail ou publicação no portal de suporte disponível através do Suporte SAP) sobre quaisquer adições ou substituições pretendidas à lista de Subcontratantes Ulteriores, incluindo o nome, endereço e função do novo Subcontratante Ulterior; e
- (b) O Cliente possa opor-se a tais alterações, conforme o definido na Secção 6.3.
- 6.3 Objeções a Novos Subcontratantes Ulteriores.**
- (a) Caso o Cliente tenha um motivo legítimo, ao abrigo da Legislação sobre Proteção de Dados, para se opor ao tratamento dos Dados Pessoais por parte do novo Subcontratante Ulterior, o Cliente poderá cessar o Contrato (de modo limitado ao Serviço Cloud para o qual se pretende utilizar o novo Subcontratante Ulterior), mediante aviso, por escrito, à SAP. Tal cessação entrará em vigor no momento determinado pelo Cliente, o mais tardar trinta dias desde a data em a SAP notificou o Cliente sobre o novo Subcontratante Ulterior. Caso o Cliente não efetive a cessação durante esse período de trinta dias, considerar-se-á que o Cliente aceitou o novo Subcontratante Ulterior.
- (b) Durante o período de trinta dias desde a data em a SAP notificou o Cliente sobre o novo Subcontratante Ulterior, o Cliente poderá solicitar um encontro entre as partes, em boa-fé, para discutir uma solução para a objeção. Tais discussões não prorrogarão o período para a cessação e não afetam o direito da SAP de utilizar o novo Subcontratante Ulterior, após esse período de trinta dias.
- (c) Qualquer cessação nos termos desta Secção 6.3 será considerada isenta de culpa por qualquer uma das partes e estará sujeita aos termos do Contrato.
- 6.4 Substituição de Urgência.** A SAP poderá substituir um Subcontratante Ulterior sem aviso prévio, quando o motivo para a alteração se encontre fora do controlo razoável da SAP e seja necessária uma substituição imediata, por motivos de segurança ou outros motivos urgentes. Nesse caso, a SAP informará o

following its appointment. Section 6.3 applies accordingly.

7. INTERNATIONAL PROCESSING

7.1 Conditions for International Processing. SAP shall be entitled to process Personal Data, including by using Subprocessors, in accordance with this DPA outside the country in which the Customer is located as permitted under Data Protection Law.

7.2 Standard Contractual Clauses. Where (i) Personal Data of an EEA or Swiss based Controller is processed in a country outside the EEA, Switzerland and any country, organization or territory acknowledged by the European Union as safe country with an adequate level of data protection under Art. 45 GDPR, or where (ii) Personal Data of another Controller is processed internationally and such international processing requires an adequacy means under the laws of the country of the Controller and the required adequacy means can be met by entering into Standard Contractual Clauses, then:

- (a)** SAP and Customer enter into the Standard Contractual Clauses;
- (b)** Customer enters into the Standard Contractual Clauses with each relevant Subprocessor as follows, either (i) Customer joins the Standard Contractual Clauses entered into by SAP or SAP SE and the Subprocessor as an independent owner of rights and obligations ("Accession Model") or, (ii) the Subprocessor (represented by SAP) enters into the Standard Contractual Clauses with Customer ("Power of Attorney Model"). The Power of Attorney Model shall apply if and when SAP has expressly confirmed that a Subprocessor is eligible for it through the Subprocessor list provided under Section 6.1(c), or a notice to Customer; and/or
- (c)** Other Controllers whose use of the Cloud Services has been authorized by Customer under the Agreement may also enter into Standard Contractual Clauses with SAP and/or the relevant Subprocessors in the same manner as Customer in accordance with Sections 7.2 (a) and (b) above. In such case, Customer will enter into the Standard Contractual Clauses on behalf of the other Controllers.

Cliente sobre o Subcontratante Ulterior de substituição logo que possível, após a sua nomeação. A Secção 6.3 aplica-se de modo correspondente.

7. TRATAMENTO INTERNACIONAL

7.1 Condições para o Tratamento Internacional. A SAP terá o direito de tratar Dados Pessoais, incluindo através da utilização de Subcontratantes Ulteriores, de acordo com o presente ATD, fora do país onde o Cliente está localizado, conforme permitido pela Legislação sobre Proteção de Dados.

7.2 Cláusulas Contratuais-tipo. Quando (i) os Dados Pessoais de um Responsável pelo Tratamento dos Dados sediado no EEE ou na Suíça sejam tratados num país fora do EEE, Suíça e qualquer país, organização ou território reconhecido pela União Europeia como um país seguro, com um nível adequado de proteção dos dados, ao abrigo do Artigo 45º do RGPD, ou quando (ii) os Dados Pessoais de outro Responsável pelo Tratamento de Dados sejam tratados internacionalmente e esse tratamento internacional requeira um esforço de adequação ao abrigo da legislação do país do Responsável pelo Tratamento de Dados, e esse esforço de adequação possa ser cumprido mediante a celebração de Cláusulas Contratuais-tipo, então:

- (a)** A SAP e o Cliente celebram as Cláusulas Contratuais-tipo;
- (b)** O Cliente celebra as Cláusulas Contratuais-tipo com cada Subcontratante Ulterior relevante, do modo seguinte: (i) o Cliente junta-se às Cláusulas Contratuais-tipo, celebradas pela SAP, ou SAP SE, e o Subcontratante Ulterior, na qualidade de um titular independente de direitos e obrigações ("Modelo de Adesão"), ou (ii) o Subcontratante Ulterior (representado pela SAP) celebra as Cláusulas Contratuais-tipo com o Cliente ("Modelo de Procuração"). O Modelo de Procuração aplicar-se-á se e quando a SAP tenha confirmado expressamente que um Subcontratante Ulterior é elegível, por meio da lista de Subcontratantes Ulteriores fornecida ao abrigo da Secção 6.1(c) ou de uma notificação ao Cliente; e/ou
- (c)** Outros Responsáveis pelo Tratamento de Dados, cuja utilização dos Serviços Cloud tenha sido autorizada pelo Cliente nos termos do Contrato, poderão igualmente celebrar as Cláusulas Contratuais-tipo com a SAP e/ou os Subcontratantes Ulteriores relevantes, do mesmo modo que o Cliente, de acordo com as Secções 7.2 (a) e (b), acima incluídas. Nesse caso, o Cliente celebrará as Cláusulas Contratuais-tipo em nome dos outros Responsáveis pelo Tratamento de Dados.

7.3 Relation of the Standard Contractual Clauses to the Agreement. Nothing in the Agreement shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses. For the avoidance of doubt, where this DPA further specifies audit and subprocessor rules in sections 5 and 6, such specifications also apply in relation to the Standard Contractual Clauses.

7.4 Governing Law of the Standard Contractual Clauses. The Standard Contractual Clauses shall be governed by the law of the country in which the relevant Controller is incorporated.

8. DOCUMENTATION; RECORDS OF PROCESSING

Each party is responsible for its compliance with its documentation requirements, in particular maintaining records of processing where required under Data Protection Law. Each party shall reasonably assist the other party in its documentation requirements, including providing the information the other party needs from it in a manner reasonably requested by the other party (such as using an electronic system), in order to enable the other party to comply with any obligations relating to maintaining records of processing.

9. EU ACCESS

9.1 Optional Service. EU Access is an optional service that may be offered by SAP. SAP shall provide the Cloud Service eligible for EU Access solely for production instances in accordance with this Section 9. Where EU Access is not expressly specified and agreed in the Order Form, this Section 9 shall not apply.

9.2 EU Access. SAP will use only European Subprocessors to provide support requiring access to Personal Data in the Cloud Service and SAP shall not export Personal Data outside of the EEA or Switzerland unless expressly authorized by Customer in writing (e-mail permitted) on a case by case basis; or as excluded under Section 9.4.

9.3 Data Center Location. Upon the effective date of the Agreement, the Data Centers used to host Personal Data in the Cloud Service are located in the EEA or Switzerland. SAP will not migrate the Customer instance to a Data Center outside the EEA or Switzerland without Customer's prior written consent (email permitted). If SAP plans to migrate the Customer instance to a Data Center within the EEA or to Switzerland, SAP will notify Customer

7.3 Relação das Cláusulas Contratuais-tipo com o Contrato. Nada no Contrato será interpretado como sendo prevalecente sobre qualquer Cláusula Contratual-tipo contraditória. Para fins de esclarecimento, quando este ATD especifique ainda regras relativas a auditorias e a subcontratantes ulteriores nas secções 5 e 6, tais especificações aplicar-se-ão também no que se refere às Cláusulas Contratuais-tipo.

7.4 Legislação Aplicável das Cláusulas Contratuais-tipo. As Cláusulas Contratuais-tipo serão reguladas pela legislação do país onde o Responsável pelo Tratamento de Dados relevante está incorporado.

8. DOCUMENTAÇÃO; REGISTOS DO TRATAMENTO

Cada uma das partes é responsável por cumprir os respetivos requisitos de documentação, em particular, mantendo registos do tratamento, quando exigido ao abrigo da Legislação sobre Proteção de Dados. Cada uma das partes ajudará, na medida do razoável, a outra parte com os requisitos de documentação, incluindo através do fornecimento de informações de que a outra parte necessita, do modo solicitado, na medida do razoável, pela outra parte (por exemplo, utilizando um sistema eletrónico), de modo a permitir que a outra parte cumpra quaisquer obrigações relativas à manutenção de registos do tratamento.

9. ACESSO DA UE

9.1 Serviço Opcional. O Acesso da UE é um serviço opcional que poderá ser oferecido pela SAP. A SAP prestará o Serviço Cloud elegível para Acesso da UE exclusivamente para instâncias produtivas, de acordo com esta Secção 9. Quando o Acesso da UE não esteja expressamente especificado e acordado no Formulário de Encomenda, esta Secção 9 não será aplicável.

9.2 Acesso da UE. A SAP utilizará apenas Subcontratantes Ulteriores Europeus para prestar suporte na solicitação de acesso a Dados Pessoais no Serviço Cloud, não podendo a SAP exportar Dados Pessoais para fora do EEE ou da Suíça, salvo se tal for expressamente autorizado, por escrito (e-mail permitido), pelo Cliente, caso a caso; ou conforme excluído nos termos da Secção 9.4.

9.3 Localização dos Centros de Tratamento de Dados ("Data Centers"). Na data de entrada em vigor do Contrato, os Centros de Tratamento de Dados utilizados para alojar Dados Pessoais no Serviço Cloud estão localizados no EEE ou na Suíça. A SAP não migrará a instância do Cliente para um Centro de Tratamento de Dados fora do EEE ou da Suíça, sem consentimento prévio, por escrito, do Cliente (e-mail permitido). Caso a SAP planeie migrar a instância do Cliente para um

in writing (email permitted) no later than thirty days before the planned migration.

9.4 Exclusions. The following Personal Data is not subject to 9.2 and 9.3:

- (a) Contact details of the sender of a support ticket; and
- (b) Any other Personal Data submitted by Customer when filing a support ticket. Customer may choose not to transmit Personal Data when filing a support ticket. If this data is necessary for the incident management process, Customer may choose to anonymize that Personal Data before any transmission of the incident message to SAP.

10. DEFINITIONS

Capitalized terms not defined herein will have the meanings given to them in the Agreement.

10.1 "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; for the purposes of this DPA, where Customer acts as processor for another controller, it shall in relation to SAP be deemed as additional and independent Controller with the respective controller rights and obligations under this DPA.

10.2 "Data Center" means the location where the production instance of the Cloud Service is hosted for the Customer in its region, as published at: <http://www.sap.com/corporate-en/about/our-company/policies/data-privacy-and-security/location-of-data-center.html> or notified to Customer or otherwise agreed in an Order Form.

10.3 "Data Protection Law" means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Agreement (and includes, as far as it concerns the relationship between the parties regarding the processing of Personal Data by SAP on behalf of Customer, the GDPR as a minimum standard, irrespective of whether the Personal Data is subject to GDPR or not).

10.4 "Data Subject" means an identified or identifiable natural person as defined by Data Protection Law.

Centro de Tratamento de Dados dentro do EEE ou da Suíça, a SAP notificará o Cliente, por escrito (e-mail permitido), no prazo máximo de trinta dias, antes da migração planeada.

9.4 Exclussões. Os seguintes Dados Pessoais não estão sujeitos a 9.2 e 9.3:

- (a) Detalhes de contacto do remetente de um pedido de suporte; e
- (b) Quaisquer outros Dados Pessoais submetidos pelo Cliente ao apresentar um pedido de suporte. O Cliente poderá optar por não transmitir Dados Pessoais ao apresentar um pedido de suporte. Caso esses dados sejam necessários para o processo de gestão de incidentes, o Cliente poderá optar por tornar esses Dados Pessoais anónimos, antes de qualquer transmissão da mensagem de incidente à SAP.

10. DEFINIÇÕES

Os termos em maiúsculas não definidos aqui terão os significados que lhes são atribuídos no Contrato.

10.1 "Responsável pelo Tratamento de Dados" designa uma pessoa singular ou jurídica, autoridade pública, agência ou outro órgão que, individualmente ou em conjunto com outros, determina as finalidades e os recursos do tratamento de Dados Pessoais; para os efeitos deste ATD, quando o Cliente atua na qualidade de subcontratante de outro responsável pelo tratamento de dados, ele será considerado, no que se refere à SAP, como um Responsável pelo Tratamento de Dados adicional e independente, com os direitos e obrigações correspondentes dessa função, nos termos do presente ATD.

10.2 "Centro de Tratamento de Dados" designa a localização onde a instância produtiva do Serviço Cloud está alojada para o Cliente na respetiva região, tal como publicado em: <http://www.sap.com/corporate-en/about/our-company/policies/data-privacy-and-security/location-of-data-center.html> ou notificado ao Cliente, ou de outro modo acordado num Formulário de Encomenda.

10.3 "Legislação sobre Proteção de Dados" designa a legislação aplicável que protege os direitos e liberdades fundamentais dos indivíduos e o seu direito à privacidade, no que se refere ao tratamento dos Dados Pessoais ao abrigo do Contrato (e inclui, desde que se refira à relação entre as partes relativamente ao tratamento de Dados Pessoais por parte da SAP em nome do Cliente, o RGPD como norma mínima, independentemente de os Dados Pessoais estarem ou não sujeitos ao RGPD).

10.4 "Titular dos Dados" designa uma pessoa singular identificada ou identificável, conforme definido pela Legislação sobre Proteção de Dados.

- 10.5 “EEA”** means the European Economic Area, namely the European Union Member States along with Iceland, Liechtenstein and Norway.
- 10.6 “European Subprocessor”** means a Subprocessor that is physically processing Personal Data in the EEA or Switzerland.
- 10.7 “Personal Data”** means any information relating to a Data Subject which is protected under Data Protection Law. For the purposes of the DPA, it includes only personal data which is (i) entered by Customer or its Authorized Users into or derived from their use of the Cloud Service, or (ii) supplied to or accessed by SAP or its Subprocessors in order to provide support under the Agreement. Personal Data is a subset of Customer Data (as defined under the Agreement).
- 10.8 “Personal Data Breach”** means a confirmed (1) accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data or (2) similar incident involving Personal Data, in each case for which a Controller is required under Data Protection Law to provide notice to competent data protection authorities or Data Subjects.
- 10.9 “Processor”** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, be it directly as processor of a controller or indirectly as subprocessor of a processor which processes personal data on behalf of the controller.
- 10.10 “Standard Contractual Clauses”** or sometimes also referred to the “EU Model Clauses” means the (Standard Contractual Clauses (processors)) or any subsequent version thereof published by the European Commission (which will automatically apply). “The Standard Contractual Clauses current as of the effective date of the Agreement are attached hereto as Appendix 4.”
- 10.11 “Subprocessor”** means SAP Affiliates, SAP SE, SAP SE Affiliates and third parties engaged by SAP, SAP SE or SAP SE’s Affiliates in connection with the Cloud Service and which process Personal Data in accordance with this DPA.
- 10.5 “EEE”** designa o Espaço Económico Europeu, nomeadamente os Estados-Membros da União Europeia, em conjunto com a Islândia, o Liechtenstein e a Noruega.
- 10.6 “Subcontratante Ulterior Europeu”** designa um Subcontratante Ulterior que trata fisicamente os Dados Pessoais no EEE ou na Suíça.
- 10.7 “Dados Pessoais”** designa quaisquer informações relativas ao Titular dos Dados que estejam protegidas ao abrigo da Legislação sobre Proteção de Dados. Para os efeitos do ATD, incluem apenas dados pessoais que (i) sejam introduzidos pelo Cliente ou respetivos Utilizadores Autorizados no Serviço Cloud ou que sejam derivados pela sua utilização do mesmo, ou (ii) sejam fornecidos à ou acedidos pela SAP ou respetivos Subcontratantes Ulteriores, de modo a fornecer suporte ao abrigo do Contrato. Os Dados Pessoais são um subconjunto dos Dados do Cliente (tal como definidos no Contrato).
- 10.8 “Violação dos Dados Pessoais”** designa (1) uma destruição, perda ou alteração acidentais ou ilícitas, ou uma divulgação de ou acesso não autorizados de terceiros a Dados Pessoais, desde que confirmados, ou (2) incidentes semelhantes que envolvam Dados Pessoais, casos em que, ao abrigo da Legislação sobre Proteção de Dados, é exigido a um Responsável pelo Tratamento de Dados que notifique as autoridades competentes para proteção de dados ou os Titulares dos Dados.
- 10.9 “Subcontratante”** designa uma pessoa singular ou jurídica, autoridade pública, agência ou outro órgão que trata dados pessoais em nome do responsável pelo tratamento de dados, quer seja diretamente como subcontratante de um responsável pelo tratamento dos dados, ou indiretamente como subcontratante ulterior de um subcontratante que trata dados pessoais em nome do responsável pelo tratamento de dados.
- 10.10 “Cláusulas Contratuais-tipo”** ou por vezes igualmente referidas como “Cláusulas-tipo da UE” designa (Cláusulas Contratuais-tipo (subcontratantes)) ou qualquer versão subsequente das mesmas, publicada pela Comissão Europeia (que será automaticamente aplicável). “As Cláusulas Contratuais-tipo, válidas a partir da data de entrada em vigor do Contrato, estão anexadas a este documento como Apêndice 4.”
- 10.11 “Subcontratante Ulterior”** designa as Filiais da SAP, a SAP SE, as Filiais da SAP SE e terceiros contratados pela SAP, SAP SE ou Filiais da SAP SE em relação ao Serviço Cloud e que tratam Dados Pessoais de acordo com este ATD.

Appendix 1 to the DPA and, if applicable, the Standard Contractual Clauses

Apêndice 1 ao ATD e, caso aplicável, às Cláusulas Contratuais-tipo

Data Exporter

The Data Exporter is the Customer who subscribed to a Cloud Service that allows Authorized Users to enter, amend, use, delete or otherwise process Personal Data. Where the Customer allows other Controllers to also use the Cloud Service, these other Controllers are also Data Exporters.

Data Importer

SAP and its Subprocessors provide the Cloud Service that includes the following support:

SAP SE Affiliates support the Cloud Service data centers remotely from SAP facilities in St. Leon/Rot (Germany), India and other locations where SAP employs personnel in the Operations/Cloud Delivery function. Support includes:

- Monitoring the Cloud Service
- Backup & restoration of Customer Data stored in the Cloud Service
- Release and development of fixes and upgrades to the Cloud Service
- Monitoring, troubleshooting and administering the underlying Cloud Service infrastructure and database
- Security monitoring, network-based intrusion detection support, penetration testing

SAP SE Affiliates provide support when a Customer submits a support ticket because the Cloud Service is not available or not working as expected for some or all Authorized Users. SAP answers phones and performs basic troubleshooting, and handles support tickets in a tracking system that is separate from the production instance of the Cloud Service.

Data Subjects

Unless provided otherwise by the Data Exporter, transferred Personal Data relates to the following categories of Data Subjects: employees, contractors, business partners or other individuals having Personal Data stored in the Cloud Service.

Data Categories

The transferred Personal Data concerns the following categories of data:

Customer determines the categories of data per Cloud Service subscribed. Customer can configure the data fields during implementation of the Cloud Service or as otherwise provided by the Cloud Service. The transferred Personal Data typically relates to the following categories of data: name, phone numbers, e-mail address, time zone, address data, system access / usage / authorization data, company name,

Exportador de Dados

O Exportador de Dados é o Cliente que subscreveu um Serviço Cloud, que permite aos Utilizadores Autorizados introduzir, emendar, utilizar, eliminar ou tratar de outro modo os Dados Pessoais. Quando o Cliente permite que outros Responsáveis pelo Tratamento de Dados também utilizem o Serviço Cloud, esses outros Responsáveis pelo Tratamento de Dados também são Exportadores de Dados.

Importador de Dados

A SAP e os respetivos Subcontratantes Ulteriores fornecem o Serviço Cloud que inclui o seguinte suporte:

As Filiais da SAP SE suportam os centros de tratamento de dados do Serviço Cloud remotamente a partir de instalações da SAP em St. Leon/Rot (Alemanha), Índia e outras localizações onde a SAP emprega pessoal que desempenha funções de Operações/Entrega Cloud. O suporte inclui:

- Controlo do Serviço Cloud
- Cópia de segurança e restauro dos Dados do Cliente armazenados no Serviço Cloud
- Lançamento e desenvolvimento de correções e upgrades para o Serviço Cloud
- Monitorização, resolução de problemas e administração da base de dados e da infraestrutura subjacente do Serviço Cloud
- Controlo de segurança, suporte de deteção de intrusões com base em rede, testes de penetração

As Filiais da SAP SE fornecem suporte quando um Cliente apresenta um pedido de suporte porque o Serviço Cloud não está disponível ou não funciona como previsto para alguns ou todos os Utilizadores Autorizados. A SAP atende chamadas, realiza resolução de problemas básicos e trata de pedidos de suporte num sistema de controlo separado da instância produtiva do Serviço Cloud.

Titulares dos Dados

Salvo se disposto de outro modo pelo Exportador de Dados, os Dados Pessoais transferidos referem-se às seguintes categorias de Titulares dos Dados: empregados, contratados, parceiros de negócios ou outros indivíduos cujos Dados Pessoais estejam armazenados no Serviço Cloud.

Categorias de Dados

Os Dados Pessoais transferidos referem-se às seguintes categorias de dados:

O Cliente determina as categorias de dados por Serviço Cloud subscrito. O Cliente pode configurar os campos de dados durante a implementação do Serviço Cloud ou tal como disposto em contrário pelo Serviço Cloud. Os Dados Pessoais transferidos habitualmente referem-se às seguintes categorias de dados: nome, números de telefone, endereço de e-mail, fuso horário, dados de endereço, dados de

contract data, invoice data, plus any application-specific data that Authorized Users enter into the Cloud Service and may include bank account data, credit or debit card data.

Special Data Categories (if appropriate)

The transferred Personal Data concerns the following special categories of data: As set out in the Agreement (including the Order Form) if any.

Processing Operations / Purposes

The transferred Personal Data is subject to the following basic processing activities:

- use of Personal Data to set up, operate, monitor and provide the Cloud Service (including Operational and Technical Support)
- provision of Consulting Services;
- communication to Authorized Users
- storage of Personal Data in dedicated Data Centers (multi-tenant architecture)
- upload any fixes or upgrades to the Cloud Service
- back up of Personal Data
- computer processing of Personal Data, including data transmission, data retrieval, data access
- network access to allow Personal Data transfer
- execution of instructions of Customer in accordance with the Agreement.

autorização/utilização/acesso ao sistema, nome da empresa, dados de contrato, dados de fatura, mais quaisquer dados específicos de aplicação que os Utilizadores Autorizados introduzem no Serviço Cloud, e poderão incluir dados de conta bancária e dados de cartão de crédito ou débito.

Categorias Especiais de Dados (caso apropriado)

Os Dados Pessoais transferidos referem-se às seguintes categorias especiais de dados: tal como definido no Contrato (incluindo o Formulário de Encomenda), caso existam.

Operações/Finalidades de Tratamento

Os Dados Pessoais transferidos estão sujeitos às seguintes atividades de tratamento básico:

- utilização dos Dados Pessoais para configurar, operar, controlar e prestar o Serviço Cloud (incluindo Suporte Técnico e Operacional)
- disponibilização de Serviços de Consultoria;
- comunicação a Utilizadores Autorizados
- armazenamento de Dados Pessoais em Centros de Tratamento de Dados dedicados (arquitetura de vários inquilinos)
- carregamento de quaisquer correções ou upgrades para o Serviço Cloud
- cópia de segurança dos Dados Pessoais
- tratamento informático dos Dados Pessoais, incluindo transmissão, obtenção e acesso aos dados
- acesso à rede para permitir a transferência dos Dados Pessoais
- execução de instruções do Cliente de acordo com o Contrato.

Appendix 2 to the DPA and, if applicable, the Standard Contractual Clauses – Technical and Organizational Measures

Apêndice 2 ao ATD e, caso aplicável, às Cláusulas Contratuais-tipo – Medidas Técnicas e Organizacionais

1. TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define SAP's current technical and organizational measures. SAP may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

1.1 Physical Access Control. Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems that process and/or use Personal Data are located.

Measures:

- SAP protects its assets and facilities using the appropriate means based on the SAP Security Policy
- In general, buildings are secured through access control systems (e.g., smart card access system).
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
- Depending on the security classification, buildings, individual areas and surrounding premises may be further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.
- Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures (see Section 1.2 and 1.3 below). This also applies to visitor access. Guests and visitors to SAP buildings must register their names at reception and must be accompanied by authorized SAP personnel.
- SAP employees and external personnel must wear their ID cards at all SAP locations.

Additional measures for Data Centers:

- All Data Centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and Data Center facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the Data Center facilities. To protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.

1. MEDIDAS TÉCNICAS E ORGANIZACIONAIS

As seções que se seguem definem as medidas técnicas e organizacionais atuais da SAP. A SAP poderá alterar estas medidas em qualquer momento sem aviso, desde que mantenha um nível de segurança comparável ou superior. Medidas individuais poderão ser substituídas por novas medidas que sirvam o mesmo propósito sem diminuir o nível de segurança que protege os Dados Pessoais.

1.1 Controlo de Acesso Físico. É impedido o acesso físico de pessoas não autorizadas às instalações, edifícios ou salas onde estão localizados os sistemas de tratamento de dados que tratam e/ou utilizam Dados Pessoais.

Medidas:

- A SAP protege os seus recursos e instalações utilizando os meios adequados, com base na Política de Segurança da SAP
- Regra geral, os edifícios são protegidos através de sistemas de controlo de acesso (por exemplo, sistema de acesso com smart card).
- Como requisito mínimo, nos pontos de acesso exterior do edifício tem de ser montado um sistema de chave certificado, que inclui uma gestão de chaves ativa e moderna.
- Dependendo da classificação de segurança, os edifícios, áreas individuais e instalações circundantes poderão estar ainda protegidos por medidas adicionais. Estas medidas incluem perfis de acesso específicos, videovigilância, sistemas de alarme de intrusão e sistemas de controlo de acesso biométricos.
- São concedidos direitos de acesso a pessoas autorizadas numa base individual, de acordo com as medidas de Controlo do Acesso a Dados e a Sistemas (consulte as Secções 1.2 e 1.3 abaixo incluídas). Isto é igualmente aplicável ao acesso de visitantes. Os convidados e visitantes dos edifícios da SAP têm de registar o seu nome na receção e ser acompanhados por pessoal da SAP autorizado.
- Os empregados e pessoal externo da SAP têm de usar os cartões de identificação em todas as localizações da SAP.

Medidas adicionais para Centros de Tratamento de Dados:

- Todos os Centros de Tratamento de Dados aderem a procedimentos de segurança rigorosos, assegurados por guardas, câmaras de vigilância, detetores de movimento, mecanismos de controlo de acesso e outras medidas para impedir que os equipamentos e as instalações de Centro de Tratamento de Dados sejam comprometidos. Apenas representantes autorizados terão acesso a sistemas e a infraestruturas nas instalações do Centro de Tratamento de Dados. Para proteger o funcionamento adequado, é realizada uma manutenção regular dos equipamentos físicos de segurança (por exemplo, sensores de movimento, câmaras, etc.).

- SAP and all third-party Data Center providers log the names and times of authorized personnel entering SAP's private areas within the Data Centers.
- Tanto a SAP como todos os prestadores externos do Centro de Tratamento de Dados registam os nomes do pessoal autorizado que entra nas áreas privadas da SAP dentro dos Centros de Tratamento de Dados, assim como as horas em que isso é efetuado.

1.2 System Access Control. Data processing systems used to provide the Cloud Service must be prevented from being used without authorization.

Measures:

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes according to the SAP Security Policy
- All personnel access SAP's systems with a unique identifier (user ID).
- SAP has procedures in place so that requested authorization changes are implemented only in accordance with the SAP Security Policy (for example, no rights are granted without authorization). In case personnel leaves the company, their access rights are revoked.
- SAP has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver.
- The company network is protected from the public network by firewalls.
- SAP uses up-to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations.
- Security patch management is implemented to provide regular and periodic deployment of relevant security updates. Full remote access to SAP's corporate network and critical infrastructure is protected by strong authentication.

1.3 Data Access Control. Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorization in the course of processing, use and storage.

Measures:

- As part of the SAP Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SAP Information Classification standard.

1.2 Controlo de Acesso ao Sistema. Tem de ser evitado que os sistemas de tratamento de dados utilizados para prestar o Serviço Cloud sejam utilizados sem autorização.

Medidas:

- São utilizados múltiplos níveis de autorização ao conceder acesso a sistemas sensíveis, incluindo aqueles que armazenam e tratam Dados Pessoais. As autorizações são administradas através de processos definidos, de acordo com a Política de Segurança da SAP
- Todo o pessoal acede aos sistemas da SAP com um identificador exclusivo (ID de utilizador).
- A SAP dispõe de procedimentos para garantir que as alterações de autorização solicitadas são implementadas exclusivamente de acordo com a Política de Segurança da SAP (por exemplo, não são outorgados quaisquer direitos sem autorização). Os direitos de acesso de pessoal que deixa a empresa são revogados.
- A SAP estabeleceu uma política de palavras-passe que proíbe a partilha de palavras-passe, regula as respostas caso uma palavra-passe seja divulgada e exige a alteração regular das palavras-passe e a modificação de palavras-passe predefinidas. São atribuídos IDs de utilizador personalizados para autenticação. Todas as palavras-passe têm de cumprir requisitos mínimos predefinidos e são armazenadas de forma encriptada. No caso de palavras-passe de domínio, o sistema força a alteração da palavra-passe a cada seis meses, que deve cumprir os requisitos para palavras-passe complexas. Cada computador tem uma proteção de ecrã protegida por palavra-passe.
- A rede da empresa está protegida da rede pública por meio de firewalls.
- A SAP utiliza software antivírus atualizado em pontos de acesso à rede da empresa (para contas de e-mail) e em todos os servidores de ficheiros e estações de trabalho.
- É implementada uma gestão de patches de segurança para fornecer implementação regular e periódica de atualizações de segurança relevantes. O acesso remoto total à rede empresarial e à infraestrutura crítica da SAP está protegido por autenticação forte.

1.3 Controlo de Acesso aos Dados. As pessoas com direito a utilizar os sistemas de tratamento de dados só terão acesso aos Dados Pessoais aos quais têm direito de aceder; os Dados Pessoais não poderão ser lidos, copiados, modificados ou removidos sem autorização, durante o tratamento, a utilização e o armazenamento.

Medidas:

- Como parte da Política de Segurança da SAP, os Dados Pessoais exigem, pelo menos, os mesmos níveis de proteção que a informação "confidencial",

- Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfill their duty. SAP uses authorization concepts that document grant processes and assigned roles per account (user ID). All Customer Data is protected in accordance with the SAP Security Policy.
- All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing Personal Data are regularly checked. To this end, SAP conducts internal and external security checks and penetration tests on its IT systems.
- SAP does not allow the installation of software that has not been approved by SAP.
- An SAP security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

1.4 Data Transmission Control. Except as necessary for the provision of the Cloud Services in accordance with the Agreement, Personal Data must not be read, copied, modified or removed without authorization during transfer. Where data carriers are physically transported, adequate measures are implemented at SAP to provide the agreed-upon service levels (for example, encryption and lead-lined containers).

Measures:

- Personal Data in transfer over SAP internal networks is protected according to SAP Security Policy.
- When data is transferred between SAP and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant agreement. This applies to both physical and network based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of SAP-controlled systems (e.g. data being transmitted outside the firewall of the SAP Data Center).

1.5 Data Input Control. It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from SAP data processing systems.

Measures:

- SAP only allows authorized personnel to access Personal Data as required in the course of their duty.
- SAP has implemented a logging system for input, modification and deletion, or blocking of Personal

de acordo com a norma de Classificação da Informação da SAP.

- O acesso a Dados Pessoais é concedido apenas se absolutamente necessário. O pessoal tem acesso à informação de que necessita para cumprir o seu dever. A SAP utiliza conceitos de autorização que documentam os processos de concessão de autorização e as funções atribuídas por conta (ID de utilizador). Todos os Dados de Cliente estão protegidos de acordo com a Política de Segurança da SAP.
- Todos os servidores de produção funcionam nos Centros de Tratamento de Dados ou em salas de servidor seguras. As medidas de segurança que protegem as aplicações para o tratamento de Dados Pessoais são verificadas regularmente. Para esse efeito, a SAP realiza verificações de segurança internas e externas e testes de penetração nos seus sistemas de IT.
- A SAP não permite a instalação de software não aprovado pela SAP.
- Um padrão de segurança da SAP regula o modo como os dados e suportes de dados são eliminados ou destruídos assim que deixam de ser necessários.

1.4 Controlo de Transmissão de Dados. Com exceção da medida necessária para a prestação dos Serviços Cloud de acordo com o Contrato, os Dados Pessoais não podem ser lidos, copiados, modificados ou removidos sem autorização durante a transferência. Quando os suportes de dados são transportados fisicamente, são implementadas na SAP medidas adequadas para fornecer os níveis de serviço acordados (por exemplo, encriptação e contentores revestidos a chumbo).

Medidas:

- Os Dados Pessoais em transferência por meio de redes internas da SAP são protegidos de acordo com a Política de Segurança da SAP.
- Quando os dados são transferidos entre a SAP e os respetivos clientes, as medidas de proteção para os Dados Pessoais transferidos são mutuamente acordadas, constituindo parte integrante do contrato relevante. Isto é aplicável tanto à transferência de dados física como à transferência baseada na rede. Em qualquer um dos casos, o Cliente assume a responsabilidade por qualquer transferência de dados, assim que esta se encontrar fora dos sistemas controlados pela SAP (por exemplo, dados transmitidos fora da firewall do Centro de Tratamento de Dados da SAP).

1.5 Controlo de Inserção de Dados. Será possível examinar e estabelecer retrospectivamente se e por quem os Dados Pessoais foram introduzidos, modificados ou removidos dos sistemas de tratamento de dados da SAP.

Medidas:

- A SAP só permite que pessoal autorizado aceda a Dados Pessoais se isso for necessário para a realização das suas obrigações.
- A SAP implementou um sistema de registo para a inserção, modificação e eliminação ou bloqueio de Dados Pessoais pela SAP ou respetivos

Data by SAP or its subprocessors within the Cloud Service to the extent technically possible.

1.6 Job Control. Personal Data being processed on commission (i.e., Personal Data processed on a customer's behalf) is processed solely in accordance with the Agreement and related instructions of the customer.

Measures:

- SAP uses controls and processes to monitor compliance with contracts between SAP and its customers, subprocessors or other service providers.
- As part of the SAP Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SAP Information Classification standard.
- All SAP employees and contractual subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of SAP customers and partners.

1.7 Availability Control. Personal Data will be protected against accidental or unauthorized destruction or loss.

Measures:

- SAP employs regular backup processes to provide restoration of business-critical systems as and when necessary.
- SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the Data Centers.
- SAP has defined business contingency plans for business-critical processes and may offer disaster recovery strategies for business critical Services as further set out in the Documentation or incorporated into the Order Form for the relevant Cloud Service.
- Emergency processes and systems are regularly tested.

1.8 Data Separation Control. Personal Data collected for different purposes can be processed separately.

Measures:

- SAP uses the technical capabilities of the deployed software (for example: multi-tenancy, or separate system landscapes) to achieve data separation among Personal Data originating from multiple customers.
- Customer (including its Controllers) has access only to its own data.
- If Personal Data is required to handle a support incident from Customer, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems.

subcontratantes ulteriores no Serviço Cloud, até ao limite máximo tecnicamente possível.

1.6 Controlo de Trabalho. Os Dados Pessoais que estão a ser tratados em comissão (isto é, Dados Pessoais tratados em nome de um cliente) são exclusivamente tratados de acordo com o Contrato e com as instruções relacionadas do cliente.

Medidas:

- A SAP utiliza controlos e processos para controlar o cumprimento dos contratos celebrados entre a SAP e os seus clientes, subcontratantes ulteriores ou outros prestadores de serviços.
- Como parte da Política de Segurança da SAP, os Dados Pessoais exigem, pelo menos, os mesmos níveis de proteção que a informação "confidencial", de acordo com a norma de Classificação da Informação da SAP.
- Todos os empregados da SAP e subcontratantes ulteriores ou outros prestadores de serviços de contrato estão vinculados contratualmente a respeitar a confidencialidade de todas as informações sensíveis, incluindo segredos comerciais dos clientes e parceiros da SAP.

1.7 Controlo de Disponibilidade. Os Dados Pessoais serão protegidos contra destruição ou perda acidentais ou não autorizadas.

Medidas:

- A SAP emprega processos de cópia de segurança regulares para fornecer o restauro dos sistemas críticos para o negócio, se e quando necessário.
- A SAP utiliza fontes de alimentação ininterruptas (UPS, baterias, geradores, etc.) para garantir que os Centros de Tratamento de Dados dispõem de energia.
- A SAP definiu planos de contingência empresariais para processos críticos para o negócio e pode oferecer estratégias de recuperação de desastres para serviços críticos, tal como definido em maior detalhe na Documentação ou incorporado no Formulário de Encomenda para o Serviço Cloud relevante.
- Os processos e sistemas de emergência são testados regularmente.

1.8 Controlo de Separação de Dados. Os Dados Pessoais recolhidos com finalidades diferentes podem ser tratados em separado.

Medidas:

- A SAP utiliza as capacidades técnicas do software implementado (por exemplo: arquitetura de vários inquilinos ou estruturas de sistemas separadas) para conseguir a separação de dados entre os Dados Pessoais de vários clientes.
- O Cliente (incluindo o respetivos Responsáveis pelo Tratamento de Dados) tem acesso apenas aos seus próprios dados.
- Se os Dados Pessoais forem necessários para tratar um incidente de suporte do Cliente, os dados serão atribuídos a essa mensagem específica e utilizados apenas para o tratamento dessa mensagem. Os dados não são acedidos para tratar quaisquer outras mensagens. Esses dados são armazenados em sistemas de suporte específicos.

1.9 Data Integrity Control. Personal Data will remain intact, complete and current during processing activities.

Measures:

SAP has implemented a multi-layered defense strategy as a protection against unauthorized modifications.

In particular, SAP uses the following to implement the control and measure sections described above:

- Firewalls;
- Security Monitoring Center;
- Antivirus software;
- Backup and recovery;
- External and internal penetration testing;
- Regular external audits to prove security measures.

1.9 Controlo de Integridade dos Dados. Os Dados Pessoais permanecerão intactos, completos e atuais durante as atividades de tratamento.

Medidas:

A SAP implementou uma estratégia de defesa em várias camadas como proteção contra modificações não autorizadas.

Em particular, a SAP utiliza o seguinte para implementar as secções sobre controlo e medidas acima descritas:

- Firewalls;
- Centro de Controlo de Segurança;
- Software antivírus;
- Cópia de segurança e recuperação;
- Testes de penetração externos e internos;
- Auditorias externas regulares para comprovar medidas de segurança.

Appendix 3 to the DPA and, if applicable, the Standard Contractual Clauses

Apêndice 3 ao ATD e, caso aplicável, às Cláusulas Contratuais-tipo

The following table sets out the relevant Articles of GDPR and corresponding terms of the DPA for illustration purposes only.

A tabela que se segue estabelece os Artigos relevantes do RGPD e termos correspondentes do ATD, apenas para fins de ilustração.

Article of GDPR	Section of DPA	Click on link to see Section
Artigo do RGPD	Secção do ATD	Clicar no link para ver a Secção
28(1)	2 and Appendix/e Apêndice 2	Segurança do Tratamento and Appendix 2, Technical and Organizational Measures. Segurança do Tratamento e Apêndice 2, Medidas Técnicas e Organizacionais.
28(2), 28(3) (d) and/e 28 (4)	6	SUBCONTRATANTES ULTERIORES SUBCONTRATANTES ULTERIORES
28 (3) sentence/frase 1	1.1 and Appendix/e Apêndice 1, 1.2	Finalidade e Aplicação. Estrutura. Finalidade e Aplicação. Estrutura.
28(3) (a) and/e 29	3.1 and/e 3.2	Instruções do Cliente. Tratamento por Requisito Legal. Instruções do Cliente. Tratamento por Requisito Legal.
28(3) (b)	3.3	Pessoal. Pessoal.
28(3) (c) and/e 32	2 and Appendix/e Apêndice 2	Segurança do Tratamento and Appendix 2, Technical and Organizational Measures. Segurança do Tratamento e Apêndice 2, Medidas Técnicas e Organizacionais.
28(3) (e)	3.4	Coopera Cooperação.
28(3) (f) and/e 32-36	2 and Appendix/e Apêndice 2, 3.5, 3.6	Segurança do Tratamento and Appendix 2, Technical and Organizational Measures. Notificação de Violação de Dados Pessoais. Data Protection Impact Assessment. Segurança do Tratamento e Apêndice 2, Medidas Técnicas e Organizacionais. Notificação de Violação de Dados Pessoais. Avaliação do Impacto da Proteção de Dados.
28(3) (g)	4	Data export and Delet Exportação e Eliminação de Dados
28(3) (h)	5	CERTIFICATION CERTIFICAÇÕES E AUDITORIAS
28 (4)	6	SUBCONTRATANTES ULTERIORES SUBCONTRATANTES ULTERIORES
30	8	Documentação; Registos do tratamento Documentação; Registos do tratamento
46(2) (c)	7.2	Standard Contractual Clauses. Cláusulas Contratuais-tipo.

Appendix 4
STANDARD CONTRACTUAL CLAUSES (PROCESSORS)¹

Apêndice 4
CLÁUSULAS CONTRATUAIS-TIPO (SUBCONTRATANTES)²

For the purposes of Article 26(2) of Directive 95/46/EC (or, after 25 May 2018, Article 44 et seq. of Regulation 2016/79) for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Para os efeitos do Artigo 26(2) da Diretiva 95/46/CE (ou, após 25 de maio de 2018, Artigo 44 e seguintes do Regulamento 2016/79) para a transferência de dados pessoais para subcontratantes estabelecidos em países terceiros que não assegurem um nível adequado de proteção dos dados

Customer also on behalf of the other Controllers
(in the Clauses hereinafter referred to as the '**data exporter**')
exporter'

Cliente, também em nome de outros Responsáveis pelo Tratamento de Dados
(doravante referido nas Cláusulas como o '**exportador de dados**')
de dados'

and

e

SAP
(in the Clauses hereinafter referred to as the '**data importer**')
importer'

SAP
(doravante referida nas Cláusulas como o '**importador de dados**')
de dados'

each a 'party'; together 'the parties',

cada um deles uma 'parte'; em conjunto 'as partes',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

ACORDARAM as seguintes Cláusulas Contratuais (as Cláusulas), de modo a apresentarem garantias adequadas, relativas à proteção da vida privada e dos direitos e liberdades fundamentais das pessoas para a transferência, pelo exportador de dados para o importador de dados, de dados pessoais especificados no Apêndice 1.

Clause 1

Cláusula 1

Definitions

Definições

For the purposes of the Clauses:

Para os efeitos das Cláusulas:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(a) 'dados pessoais', 'categorias especiais de dados', 'tratamento', 'responsável pelo tratamento', 'subcontratante', 'titular dos dados' e 'autoridade fiscalizadora' terão o mesmo significado que o estipulado na Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995, sobre a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados;

(b) 'the data exporter' means the controller who transfers the personal data;

(b) 'o exportador de dados' designa o responsável pelo tratamento que transfere os dados pessoais;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(c) 'o importador de dados' designa o subcontratante que aceita receber, do exportador de dados, dados pessoais para tratamento em seu nome após a transferência, de acordo com as suas instruções e com os termos das Cláusulas, e que não está sujeito a que o sistema de um país terceiro assegure a proteção adequada na aceção do Artigo 25(1) da Diretiva 95/46/CE;

¹ Pursuant to Commission Decision of 5 February 2010 (2010/87/EU)

² Nos termos da Decisão da Comissão de 5 de fevereiro de 2010 (2010/87/UE)

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have

(d) 'o subcontratante ulterior' designa qualquer subcontratante, contratado pelo importador de dados ou por qualquer outro dos seus subcontratantes ulteriores, que aceita receber do importador de dados ou de qualquer outro dos seus subcontratantes ulteriores, dados pessoais exclusivamente para atividades de tratamento a efetuar em nome do exportador de dados após a transferência, de acordo com as suas instruções, com os termos das Cláusulas e com os termos do subcontrato escrito;

(e) 'a legislação aplicável sobre proteção de dados' designa a legislação que protege os direitos e liberdades fundamentais das pessoas e, em particular, o seu direito à vida privada no que se refere ao tratamento de dados pessoais, aplicável a um responsável pelo tratamento de dados no Estado-Membro em que o exportador de dados está estabelecido;

(f) 'medidas de segurança técnicas e organizacionais' designa as medidas que têm por objetivo proteger os dados pessoais contra destruição acidental ou ilícita, perda acidental, alteração, divulgação ou acesso não autorizados, nomeadamente quando o tratamento implicar a transmissão de dados através de uma rede, e contra qualquer outra forma de tratamento ilícito.

Cláusula 2

Detalhes da transferência

Os detalhes da transferência e, em particular, as categorias especiais de dados pessoais, quando aplicável, estão especificados no Apêndice 1, que constitui parte integrante das Cláusulas.

Cláusula 3

Cláusula do terceiro beneficiário

1. O titular dos dados pode fazer aplicar, contra o exportador de dados, a presente Cláusula, a Cláusula 4(b) a (i), a Cláusula 5(a) a (e), e (g) a (j), a Cláusula 6(1) e (2), a Cláusula 7, a Cláusula 8(2) e as Cláusulas 9 a 12, como terceiro beneficiário.

2. O titular dos dados pode fazer aplicar, contra o importador de dados, a presente Cláusula, a Cláusula 5(a) a (e) e (g), a Cláusula 6, a Cláusula 7, a Cláusula 8(2) e as Cláusulas 9 a 12, em caso de desaparecimento de facto ou de extinção legal do exportador de dados, a menos que qualquer entidade sucessora tenha assumido a totalidade das obrigações legais do exportador de dados mediante contrato ou por força da lei, e consequentemente assumida os direitos e obrigações do exportador de dados, podendo nesse caso o titular dos dados fazê-las aplicar contra tal entidade.

3. O titular dos dados pode fazer aplicar, contra o subcontratante ulterior, a presente Cláusula, a Cláusula 5(a) a (e) e (g), a Cláusula 6, a Cláusula 7, a Cláusula 8(2) e as Cláusulas 9 a 12, em caso de desaparecimento

factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer

de facto ou de extinção legal tanto do exportador de dados como do importador de dados, ou se esses se tornarem insolventes, a menos que qualquer entidade sucessora tenha assumido a totalidade das obrigações legais do exportador de dados mediante contrato ou por força da lei, e conseqüentemente assumam os direitos e obrigações do exportador de dados, podendo nesse caso o titular dos dados fazê-las aplicar contra tal entidade. Essa responsabilidade civil do subcontratante ulterior será limitada às suas próprias atividades de tratamento ao abrigo das Cláusulas.

4. As partes não se opõem a que um titular dos dados seja representado por uma associação ou outro organismo se, expressamente, assim o desejar e a legislação nacional o permitir.

Cláusula 4

Obrigações do exportador de dados

O exportador de dados aceita e garante:

(a) que o tratamento dos dados pessoais, incluindo a própria transferência, foi e continuará a ser feito de acordo com as disposições pertinentes da legislação aplicável sobre proteção de dados (e que, se aplicável, foi notificado às entidades competentes do Estado-Membro em que o exportador de dados está estabelecido) e que não viola as disposições pertinentes desse Estado;

(b) que deu e continuará a dar instruções ao importador de dados, durante os serviços de tratamento de dados pessoais, para tratar os dados pessoais transferidos apenas por conta do exportador de dados e em conformidade com a legislação aplicável sobre proteção de dados e com as Cláusulas;

(c) que o importador de dados oferecerá garantias suficientes em relação às medidas de segurança técnicas e organizacionais especificadas no Apêndice 2 do presente contrato;

(d) que, depois de avaliar os requisitos da legislação aplicável sobre proteção de dados, as medidas de segurança são adequadas para proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a alteração, a divulgação ou o acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão através de uma rede, e contra qualquer outra forma de tratamento ilícito, e que estas medidas asseguram um nível de segurança adequado em relação aos riscos que o tratamento representa e à natureza dos dados a proteger, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação;

(e) que assegurará o cumprimento das medidas de segurança;

(f) que, se a transferência envolver categorias especiais de dados, o titular dos dados foi informado ou será informado antes ou o mais depressa possível após

that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

a transferência, de que os seus dados poderão ser transmitidos para um país terceiro que não garante a proteção adequada na aceção da Diretiva 95/46/CE;

(g) que enviará qualquer notificação recebida do importador de dados ou de qualquer subcontratante ulterior à autoridade fiscalizadora responsável pela proteção dos dados, nos termos da Cláusula 5(b) e da Cláusula 8(3), se o exportador de dados decidir continuar a transferência ou levantar a suspensão;

(h) que disponibilizará aos titulares dos dados, mediante pedido, uma cópia das Cláusulas, com exceção do Apêndice 2, e uma descrição sumária das medidas de segurança, bem como uma cópia de qualquer contrato de serviços de subcontratação ulterior que tenha de ser celebrado em conformidade com as Cláusulas, a menos que estas ou o contrato contenham informações comerciais, caso em que poderá remover essas informações;

(i) que, em caso de subcontratação ulterior, a atividade de tratamento é realizada em conformidade com a Cláusula 11 por um subcontratante ulterior que assegure pelo menos o mesmo nível de proteção dos dados pessoais e dos direitos do titular dos dados que o importador de dados em conformidade com as Cláusulas; e

(j) que assegurará o cumprimento da Cláusula 4(a) a (i).

Cláusula 5

Obrigações do importador de dados

O importador de dados aceita e garante:

(a) que tratará os dados pessoais apenas em nome do exportador de dados e em conformidade com as suas instruções e as Cláusulas; no caso de não poder cumprir estas obrigações por qualquer razão, concorda em informar imediatamente o exportador de dados desse facto, tendo neste caso o exportador de dados o direito de suspender a transferência de dados e/ou de cessar o contrato;

(b) que não tem qualquer razão para crer que a legislação que lhe é aplicável o impede de respeitar as instruções recebidas do exportador de dados e as obrigações que lhe incumbem por força do contrato e que, no caso de haver uma alteração nesta legislação que possa ter um efeito adverso substancial nas garantias e obrigações conferidas pelas Cláusulas, notificará imediatamente essa alteração ao exportador de dados, logo que dela tiver conhecimento, tendo neste caso o exportador de dados o direito de suspender a transferência de dados e/ou de cessar o contrato;

(c) que aplicou as medidas de segurança técnicas e organizacionais previstas no Apêndice 2 antes de tratar os dados pessoais transferidos;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any

(d) que notificará imediatamente o exportador de dados no que respeita a:

(i) qualquer pedido juridicamente vinculativo de divulgação dos dados pessoais por parte de uma autoridade competente para a aplicação da lei, a não ser que exista uma proibição em contrário, como uma proibição prevista no direito penal para preservar a confidencialidade de uma investigação policial;

(ii) qualquer acesso accidental ou não autorizado; e

(iii) qualquer pedido recebido diretamente dos titulares dos dados, sem responder a esse pedido, a não ser que tenha sido autorizado a fazê-lo;

(e) que responderá rápida e adequadamente a todos os pedidos de informação do exportador de dados relacionados com o tratamento por si efetuado dos dados pessoais objeto da transferência e que se submeterá aos conselhos da autoridade fiscalizadora relativamente ao tratamento dos dados transferidos;

(f) que, a pedido do exportador de dados, apresentará as suas instalações de tratamento de dados para auditoria das atividades de tratamento abrangidas pelas Cláusulas, que será efetuada pelo exportador de dados ou por um organismo de inspeção, composto por membros independentes que possuam as qualificações profissionais exigidas e estejam vinculados por um dever de confidencialidade, escolhido pelo exportador de dados e, se necessário, de acordo com a autoridade fiscalizadora;

(g) que disponibilizará ao titular dos dados, mediante pedido, uma cópia das Cláusulas ou de qualquer contrato existente de subcontratação ulterior, a menos que as Cláusulas ou o contrato contenham informações comerciais, caso em que poderá remover as informações comerciais, com exceção do Apêndice 2, que será substituído por uma descrição sumária das medidas de segurança, no caso de o titular dos dados não poder obter uma cópia do exportador de dados;

(h) que, em caso de subcontratação ulterior, informou previamente o exportador de dados e obteve o seu consentimento escrito prévio;

(i) que os serviços de tratamento de dados efetuados pelo subcontratante ulterior serão prestados em conformidade com a Cláusula 11;

(j) que enviará rapidamente ao exportador de dados uma cópia de qualquer contrato de subcontratação ulterior que celebrar ao abrigo das Cláusulas.

Cláusula 6

Responsabilidade

1. As partes aceitam que qualquer titular dos dados que tenha sofrido danos resultantes de qualquer incumprimento das obrigações referidas nas Cláusulas 3

party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or

ou 11, por qualquer parte ou subcontratante ulterior, tem o direito de obter reparação do exportador de dados pelos danos sofridos.

2. Se o titular dos dados não puder intentar uma ação de reparação em conformidade com o parágrafo 1 contra o exportador de dados, por incumprimento pelo importador de dados ou o seu subcontratante ulterior de quaisquer das suas obrigações referidas nas Cláusulas 3 ou 11, devido ao desaparecimento de facto ou extinção legal ou à insolvência do exportador de dados, o importador de dados aceita que o titular dos dados lhe possa intentar uma ação como se fosse o exportador de dados, a menos que qualquer entidade sucessora tenha assumido a totalidade das obrigações legais do exportador de dados, mediante contrato ou por força da lei, caso em que o titular dos dados pode invocar os seus direitos contra essa entidade.

O importador de dados não pode invocar o incumprimento da parte de um subcontratante ulterior das suas obrigações para se eximir às suas próprias responsabilidades.

3. Se um titular dos dados não puder intentar a ação referida nos parágrafos 1 e 2 contra o exportador ou o importador de dados, por incumprimento por parte do subcontratante ulterior de quaisquer das suas obrigações referidas nas Cláusulas 3 ou 11, devido ao desaparecimento de facto ou extinção legal ou à insolvência do exportador e do importador de dados, o subcontratante ulterior aceita que o titular dos dados lhe possa intentar uma ação relativamente às suas próprias atividades de tratamento de dados ao abrigo das Cláusulas, como se fosse o exportador ou o importador de dados, a menos que qualquer entidade sucessora tenha assumido a totalidade das obrigações legais do exportador ou do importador de dados, mediante contrato ou por força da lei, caso em que o titular dos dados pode invocar os seus direitos contra essa entidade. A responsabilidade do subcontratante ulterior será limitada às suas próprias atividades de tratamento de dados ao abrigo das Cláusulas.

Cláusula 7

Mediação e jurisdição

1. O importador de dados aceita que se o titular dos dados invocar contra ele os direitos de terceiro beneficiário e/ou exigir uma indemnização por danos nos termos das Cláusulas, o importador de dados aceitará a decisão do titular dos dados de:

(a) submeter o litígio a mediação de uma pessoa independente ou, quando aplicável, da autoridade fiscalizadora;

(b) submeter o litígio aos tribunais do Estado-Membro em que o exportador de dados está estabelecido.

2. As partes aceitam que a opção do titular dos dados não prejudicará os direitos materiais ou

procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

processuais do mesmo de obter reparação em conformidade com outras disposições do direito nacional ou internacional.

Cláusula 8

Cooperação com as autoridades fiscalizadoras

1. O exportador de dados aceita depositar uma cópia deste contrato junto da autoridade fiscalizadora se esta o solicitar ou se a legislação sobre proteção de dados aplicável assim o exigir.

2. As partes aceitam que a autoridade fiscalizadora tem o direito de realizar auditorias ao importador de dados e a qualquer subcontratante ulterior, com o mesmo âmbito e nas mesmas condições das auditorias efetuadas ao exportador de dados, em conformidade com a legislação aplicável sobre proteção de dados.

3. O importador de dados notificará imediatamente o exportador de dados da existência de legislação que lhe é aplicável ou a qualquer subcontratante ulterior e que impede a realização de uma auditoria ao importador de dados ou a qualquer subcontratante ulterior, nos termos do parágrafo 2. Nesse caso, o exportador de dados terá o direito de adotar as medidas previstas na Cláusula 5(b).

Cláusula 9

Legislação aplicável

As Cláusulas serão regidas pela legislação do Estado-Membro onde o exportador de dados está estabelecido.

Cláusula 10

Alteração do contrato

As partes comprometem-se a não alterar ou modificar as Cláusulas. Tal não impede que as partes aditem cláusulas de carácter comercial sempre que necessário, desde que as mesmas não contrariem a Cláusula.

Cláusula 11

Subcontratação ulterior

1. O importador de dados não subcontratará nenhuma das suas atividades de tratamento executadas em nome do exportador de dados nos termos das Cláusulas sem o consentimento escrito prévio deste. Sempre que o importador de dados subcontratar as suas obrigações nos termos das presentes Cláusulas, com o consentimento do exportador de dados, fá-lo-á apenas mediante contrato por escrito com o subcontratante ulterior que imponha a este último as mesmas obrigações do importador de dados ao abrigo das Cláusulas. Em caso de incumprimento pelo subcontratante ulterior das obrigações em matéria de proteção de dados que lhe incumbem nos termos do referido contrato escrito, o importador de dados continuará a ser plenamente responsável perante o

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

exportador de dados pelo cumprimento destas obrigações do subcontratante ulterior ao abrigo do referido contrato.

2. O contrato escrito prévio entre o importador de dados e o subcontratante ulterior deve prever igualmente uma cláusula do terceiro beneficiário, tal como previsto na Cláusula 3, para os casos em que o titular dos dados não puder intentar a ação de reparação referida no parágrafo 1 da Cláusula 6, contra o exportador ou o importador de dados por estes terem desaparecido de facto ou terem sido extintos legalmente ou por se terem tornado insolventes e nenhuma entidade sucessora ter assumido a totalidade das obrigações do exportador ou do importador de dados, mediante contrato ou por força da lei. Essa responsabilidade civil do subcontratante ulterior será limitada às suas próprias atividades de tratamento de dados nos termos das presentes Cláusulas.

3. As disposições relativas aos aspetos ligados à proteção de dados no que se refere à subcontratação ulterior do contrato referido no parágrafo 1 serão regidas pela legislação do Estado-Membro onde o exportador de dados está estabelecido.

4. O exportador de dados manterá uma lista dos contratos de subcontratação ulterior celebrados ao abrigo das Cláusulas e notificados pelo importador de dados em conformidade com a cláusula 5(j), que será atualizada pelo menos uma vez por ano. A lista será colocada à disposição da autoridade fiscalizadora da proteção de dados do exportador de dados.

Clause 12

Cláusula 12

Obligation after the termination of personal data-processing services

Obrigaçãõ depois de terminados os serviços de tratamento de dados pessoais

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

1. As partes aceitam que, após terminada a prestação de serviços de tratamento de dados, o importador de dados e o subcontratante ulterior, conforme preferência do exportador de dados, devolverão todos os dados pessoais transferidos e as suas cópias ao exportador de dados ou destruirão todos os dados pessoais e certificarão ao exportador de dados que o fizeram, exceto se a legislação imposta ao importador de dados o impedir de devolver ou destruir a totalidade ou parte dos dados pessoais transferidos. Nesse caso, o importador de dados garante a confidencialidade dos dados pessoais transferidos e não voltará a tratar ativamente os dados pessoais transferidos.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

2. O importador de dados e o subcontratante ulterior garantem que, a pedido do exportador de dados e/ou da autoridade fiscalizadora, submeterão as suas instalações de tratamento de dados a uma auditoria das medidas referidas no parágrafo 1.