CONTRATO DE PROCESSAMENTO DE DADOS (CPD)

Este Contrato de Processamento de Dados ("**CPD**") reflete o acordo das partes com relação aos termos que regem o Processamento de Dados Pessoais em nome do Cliente sob qualquer acordo escrito aplicável entre o Cliente e a Dynatrace que rege o uso das Ofertas da Dynatrace (pagas ou não) e quaisquer formulários de pedido anexos e declarações de trabalho relacionados (coletivamente denominado "**Contrato**"). Este CPD entra em vigor na data em que foi assinado por ambas as partes (e possui a "**Data de Vigência**").

Este CPD está sujeito aos termos, é totalmente incorporado e faz parte do Contrato. Este CPD substituirá qualquer acordo de processamento de dados existente, salvo indicação explícita em contrário aqui. No caso de qualquer conflito entre este CPD e qualquer outra disposição do Contrato com relação aos dados pessoais, este CPD regerá e será aplicado. Os termos em letras maiúsculas usados, mas não definidos neste CPD, têm os mesmos significados estabelecidos no Contrato de Assinatura disponível em https://assets.dynatrace.com/global/legal/Online-SA-April-2023-Portuguese-Brazilian.pdf

1. **Definições.**

   (a) "**APPI**" significa a Lei Japonesa sobre a Proteção de Informações Pessoais (Lei nº 57 de 2003, conforme alterada em 2016

   (b) "**Lei de Proteção de Dados**" significa todas as leis e regulamentos de proteção de dados e privacidade de dados aplicáveis ao Processamento de Dados Pessoais do Cliente pela Dynatrace nos termos do Contrato.

   (c) "**Controller**" tem o mesmo significado atribuído pela Lei de Proteção de Dados aplicável e inclui "Proprietário do Banco de Dados" sob a Lei de Proteção de Privacidade de Israel e "Empresa" sob a Lei de Privacidade do Estado dos EUA aplicável

   (d) "**Dados Pessoais do Cliente**" significa quaisquer Dados Pessoais enviados, armazenados, publicados, exibidos ou de outra forma transmitidos por ou em nome do Cliente durante o uso das Ofertas da Dynatrace; e exclui Dados Pessoais (como Informações Restritas) enviados, armazenados, publicados, exibidos ou de outra forma transmitidos por ou em nome do Cliente, em violação de qualquer disposição do Contrato e/ou deste CPD.

   (e) "**Dynatrace Group**" significa um ou mais da Dynatrace LLC, uma sociedade de responsabilidade limitada de Delaware, e suas Afiliadas que podem ajudar a Dynatrace a fornecer as Ofertas da Dynatrace e/ou suporte ou serviços relacionados, nos termos do Contrato e deste CPD.

   (f) "**Europa**" significa a União Europeia, o Espaço Económico Europeu ("EEE") e/ou os seus estados membros, a Suíça e o Reino Unido.

   (g) "**GDPR**" significa o Regulamento 2016/679 do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados).

   (h) "**LGPD**" significa a Lei Geral de Proteção de Dados Pessoais (Lei Geral de Proteção de Dados Pessoais no Brasil).

   (i) "**Violação de Dados Pessoais"** significa uma violação de segurança que leva à destruição, perda, alteração ou divulgação acidental ou ilegal, ou acesso não autorizado, aos Dados Pessoais do Cliente enquanto são transmitidos, armazenados ou de outra forma Processados pela Dynatrace.

   (j) "**PIPL**" significa a Lei de Proteção de Informações Pessoais da China.

   (k) "**Dados Pessoais"** significa **"Dados Pessoais"** ou **"Informações Pessoais"** conforme definido nas Leis

de Proteção de Dados aplicáveis que a Dynatrace coleta ou recebe em nome do Cliente. Os Dados Pessoais não incluem informações que a Dynatrace obtém ou processa independentemente do desempenho de suas respectivas obrigações nos termos do Contrato com o Cliente.

(l) "**Processo**r" tem o mesmo significado atribuído pela Lei de Proteção de Dados aplicável e inclui "Titular" conforme definido na Lei de Proteção de Privacidade de Israel, e "Provedor de Serviços" de acordo com a Lei de Privacidade do Estado dos EUA aplicável.

(m) "**Cláusulas Contratuais Padrão"** significa as Cláusulas Contratuais Padrão promulgadas pela Decisão 2021/914/UE da Comissão da UE incorporadas neste documento por referência, conforme atualizadas, alteradas ou substituídas de tempos em tempos.

(n) "**Sub-processador**" significa Processadores contratados pela Dynatrace ou membros do Grupo Dynatrace para permitir que a Dynatrace entregue/forneça as Ofertas da Dynatrace sob os termos do Contrato ou deste CPD.

(o) "**Autoridade Supervisora"** significa a agência governamental, departamento ou outra organização competente com autoridade sobre o processamento de Dados Pessoais relevantes para este APD.

(p) "**Adendo do Reino Unido"** significa o Adendo de Transferência Internacional de Dados às Cláusulas Contratuais Padrão da Comissão da UE emitidas pelo escritório do Comissário de Informação do Reino Unido sob S119A (1) Lei de Proteção de Dados de 2018, conforme atualizado, alterado ou substituído de tempos em tempos.

(q) **"Empresa"**, **"Controlador"**, **"Consumidor"**, **"Processador"**, **"Provedor de Serviços"**, **"Titular dos Dados", "Venda",** e **"Processamento"** (e **"processo"**) deverão ter os significados dados na Lei de Proteção de Dados aplicável.

2. Aplicabilidade da CPD e das funções das partes

(a) Este CPD se aplica ao Processamento de Dados Pessoais do Cliente pela Dynatrace em nome do Cliente para cumprir suas obrigações e exercer seus direitos sob o Contrato e este CPD. Para evitar dúvidas, este CPD não se aplica ao Processamento de Dados Pessoais do Cliente pela Dynatrace como Controladora.

(b) O Cliente é um Controlador ou Processador e a Dynatrace é um Processador. Na medida aplicável sob a Lei de Proteção de Dados, o Cliente nomeia a Dynatrace como Processadora para processar os Dados Pessoais do Cliente em nome do Cliente.

3. Tratamento de Dados Pessoais do Cliente

(a) A natureza e a extensão do Processamento de Dados Pessoais do Cliente pela Dynatrace para entregar as Ofertas da Dynatrace são determinadas e controladas pelo Cliente e são complementadas pelo Anexo A. A natureza, finalidade e duração do Processamento, bem como os tipos de Dados Pessoais coletados e as categorias de titulares de dados cujos dados pessoais podem ser processados pela Dynatrace estão descritos no Anexo A deste CPD. O Cliente reconhece que a Dynatrace não tem qualquer conhecimento dos dados reais ou dos tipos de Dados Pessoais contidos nos Dados do Cliente. As partes concordam que as instruções completas e finais do Cliente sobre a natureza e os propósitos do Processamento em conexão com as Ofertas da Dynatrace estão definidas no Contrato e neste CPD.

(b) Quaisquer alterações ou modificações nas instruções serão comunicadas por escrito e reconhecidas por ambas as partes. A Dynatrace informará o Cliente se, em sua opinião razoável, as instruções de processamento do Cliente forem susceptíveis de infringir qualquer Lei de Proteção de Dados aplicável; nesse caso, a Dynatrace tem o direito de recusar o Processamento de Dados Pessoais do Cliente que acredita estar violando qualquer Lei de Proteção de Dados aplicável até que o Cliente altere suas instruções para não estar infringindo.

(c) Na medida em que a configuração das Ofertas da Dynatrace pelo Cliente resulte na captura de Dados Pessoais do Cliente pela Dynatrace, o Cliente declara e garante que, em todos os momentos, cumprirá todas as Leis de Proteção de Dados aplicáveis. Assim como entre o Cliente e a Dynatrace, o Cliente é responsável por: (i) proteger os Dados Pessoais do Cliente durante o uso da Dynatrace, definindo as Configurações de Privacidade de Dados da Dynatrace conforme descrito em https://docs.dynatrace.com/docs/manage/data-privacy-and-security (instruções da Dynatrace sobre como definir as configurações de privacidade de dados) para controlar gradualmente o escopo dos Dados Pessoais do Cliente a serem capturados pelas Ofertas da Dynatrace; (ii) a exatidão, qualidade e legalidade dos Dados Pessoais do Cliente e os meios pelos quais o Cliente ou qualquer terceiro relevante adquiriu Dados Pessoais.

(d) Se o Cliente for um processador agindo em nome de um Controlador terceirizado, o Cliente garante à Dynatrace que as instruções e ações do Cliente com relação a esses Dados Pessoais do Cliente, incluindo a nomeação da Dynatrace como outro Processador, foram autorizadas pelo respectivo Controlador.

(e) O Cliente declara e garante que: (i) informará seus Titulares dos Dados, conforme exigido por lei, sobre o uso de Processadores para Processar Dados Pessoais de seus Cliente, incluindo a Dynatrace, incluindo, quando necessário, o fornecimento de notificação aos Titulares dos Dados sobre o uso das Ofertas da Dynatrace; (ii) obteve e continuará a ter, durante o prazo determinado, todos os direitos necessários, bases legais, autorizações e/ou consentimentos válidos, inclusive dos Titulares dos Dados, para o Processamento de Dados Pessoais de seus Cliente pela Dynatrace, conforme contemplado pelo Contrato; (iii) O uso das Ofertas da Dynatrace pelo Cliente não violará, e nem fará com que a Dynatrace viole, nenhuma Lei de Proteção de Dados aplicável ou outras leis ou regulamentos aplicáveis, nem causará uma violação de qualquer contrato ou obrigação entre o Cliente e qualquer terceiro.

(f) O Cliente fornecerá à Dynatrace apenas os Dados Pessoais do Cliente necessários para que a Dynatrace cumpra suas obrigações nos termos do Contrato com relação às Ofertas da Dynatrace e quaisquer serviços relacionados. O Cliente reconhece que o uso das Ofertas da Dynatrace não exige e não é adequado para o Processamento de quaisquer Informações Restritas e não fornecerá, por meio do uso das Ofertas da Dynatrace, quaisquer Informações Restritas a serem processadas pela Dynatrace.

4. Solicitações de Terceiros.

(a) As Ofertas da Dynatrace fornecem ao Cliente funcionalidade para acessar os Dados Pessoais do Cliente, a fim de auxiliar os Clientes com solicitações de Titulares de Dados que exercem seus direitos concedidos a eles sob a Lei de Proteção de Dados (“Solicitações de Titulares de Dados”) ou solicitações de órgãos reguladores ou judiciais relacionados ao Processamento de Dados Pessoais do Cliente. Na medida em que o Cliente não consiga acessar os Dados Pessoais do Cliente relevantes nas Ofertas da Dynatrace ou o acesso aos Dados Pessoais do Cliente não forneça assistência suficiente para responder a tais solicitações de acordo com a Lei de Proteção de Dados e, quando exigido pela Lei de Proteção de Dados aplicável, a Dynatrace concorda, a pedido do Cliente, em fornecer assistência razoável ao Cliente, para permitir que o Cliente responda às Solicitações do Titular dos Dados ou às solicitações de órgãos reguladores ou judiciais relacionadas ao Processamento de Dados Pessoais do Cliente nos termos do Contrato. Se uma solicitação for feita diretamente à Dynatrace relativa aos Dados Pessoais do Cliente para os quais a Dynatrace possa identificar o Cliente como o Controlador, a Dynatrace encaminhará, sem demora injustificada, tal comunicação ao Cliente e não responderá a tal solicitação sem a autorização expressa do Cliente. O acima exposto não proibirá a Dynatrace de se comunicar com um Titular dos Dados ou órgão regulador ou judicial se não for razoavelmente aparente na comunicação que a solicitação está relacionada ao Cliente ou se a Dynatrace tiver a obrigação legal de responder por si mesma.

(b) Se a Dynatrace for obrigada a divulgar Dados Pessoais dos quais o Cliente é o Controlador devido a uma solicitação de uma agência de aplicação da lei ou outro terceiro, a Dynatrace notificará o Cliente de tal solicitação antes de conceder acesso e/ou fornecer Dados Pessoais, para permitir que o Cliente busque uma ordem de proteção ou outra solução apropriada. Se a Dynatrace for legalmente proibida de fornecer

aviso ao Cliente, a Dynatrace tomará medidas para proteger os Dados Pessoais contra divulgação indevida, como se fossem as Informações Confidenciais da própria Dynatrace sendo solicitadas.

5. **Assistência e Cooperação**. Sujeito à natureza do processamento e aos Dados Pessoais disponíveis para a Dynatrace e quando exigido pela Lei de Proteção de Dados aplicável, a Dynatrace irá, mediante solicitação por escrito do Cliente, fornecer assistência e informações razoáveis ao Cliente, onde, a critério do Cliente, o tipo de Processamento realizado pela Dynatrace exige uma avaliação de impacto na proteção de dados e/ou consulta prévia com as autoridades de proteção de dados relevantes e fornece assistência razoável ao Cliente no cumprimento de suas outras obrigações sob a Lei de Proteção de Dados aplicável relativa à segurança de dados e notificações de violação de dados pessoais, na medida em que aplicável ao Processamento de Dados Pessoais do Cliente. O Cliente reembolsará a Dynatrace por todos os custos não negligenciáveis incorridos pela Dynatrace no cumprimento de suas obrigações sob esta seção.

6. **Conformidade demonstrável.** A Dynatrace concorda em fornecer as informações necessárias para demonstrar a conformidade com este CPD mediante solicitação razoável do Cliente.

7. **Auditorias e Avaliações.**

(a) Quando as Leis de Proteção de Dados aplicáveis concederem ao Cliente um direito de auditoria ou avaliação e sujeito ao escopo de tal direito, o Cliente poderá realizar, mediante solicitação por escrito do Cliente e até uma vez por ano, uma auditoria ou avaliação das políticas, procedimentos, e registros relevantes para o Processamento de Dados Pessoais do Cliente, de acordo com as Leis de Proteção de Dados aplicáveis.

(b) Para solicitar uma auditoria, o Cliente deve enviar à Dynatrace um plano de auditoria detalhado com pelo menos quatro (4) semanas de antecedência da data de auditoria proposta, cujo plano descreve o escopo proposto, a duração e a data de início da auditoria. A Dynatrace revisará o plano de auditoria e fornecerá ao Cliente quaisquer preocupações ou dúvidas. Antes do início de qualquer auditoria, as partes deverão chegar a acordo sobre um plano de auditoria detalhado, incluindo honorários, calendário, âmbito dos controlos, provas a serem produzidas e duração. Se o escopo de auditoria solicitado for abordado em um relatório de auditoria semelhante nos últimos doze meses e a Dynatrace confirmar que não há alterações materiais nos controles auditados, o Cliente concorda em aceitar essas descobertas em vez de solicitar uma auditoria dos controles cobertos pelo relatório

(c) Qualquer auditoria ou avaliação deverá ser: (i) conduzida durante o horário comercial normal da Dynatrace; (ii) sujeito às obrigações de confidencialidade das partes. Se um terceiro conduzir a auditoria, o terceiro não deverá ser um concorrente da Dynatrace e estará sujeito ao consentimento prévio da Dynatrace e deverá assinar um acordo de confidencialidade por escrito com as partes antes de conduzir a auditoria.

(d) Quaisquer auditorias serão por conta do Cliente. Qualquer solicitação para que a Dynatrace forneça assistência com uma auditoria será considerada um serviço separado se tal assistência de auditoria exigir o uso de recursos diferentes ou adicionais aos necessários para o fornecimento das Ofertas da Dynatrace. A Dynatrace buscará a confirmação por escrito do Cliente de que pagará quaisquer taxas aplicáveis antes de realizar tal assistência de auditoria.

8. **Confidencialidade**. A Dynatrace garantirá que qualquer pessoa autorizada a processar os Dados Pessoais do Cliente (incluindo seus funcionários, agentes e subcontratados) estará sujeita a um dever contratual, legal ou outras obrigações vinculativas de confidencialidade.

9. **Segurança**

(a) **Medidas de segurança.** Tendo em conta todo o “estado da arte”, os custos de implementação e a natureza, o âmbito, o contexto e as finalidades do Tratamento, bem como o risco de probabilidade e gravidade variáveis para os direitos e liberdades das pessoas singulares, a Dynatrace implementou e manterá medidas adequadas medidas técnicas e organizacionais destinadas a fornecer um nível de segurança

adequado ao risco de Processamento de Dados Pessoais do Cliente **("Medidas de Segurança")**. O Cliente confirma que a implementação das Medidas de Segurança identificadas no **Anexo B** pela Dynatrace é suficiente para fins de cumprimento de suas obrigações sob este CPD. Não obstante o acima exposto, o Cliente reconhece e concorda que é responsável pelo seu próprio uso seguro das Ofertas da Dynatrace

(b) **Violação de Dados Pessoais.** Assim tomar conhecimento de uma Violação de Dados Pessoais, exigida a Dynatrace, relacionada a Lei de Proteção de Dados aplicável, a Dynatrace notificará o Cliente o mais rápido possível ou sem demora injustificada. A Dynatrace iniciará imediatamente uma investigação sobre as circunstâncias que envolvem a Violação de Dados Pessoais e disponibilizará suas descobertas ao Cliente. A Dynatrace se esforçará para tomar todas as medidas exigidas pela Lei de Proteção de Dados aplicável para mitigar os efeitos de tal Violação de Dados Pessoais. A pedido do Cliente e levando em consideração a natureza do Processamento e as informações disponíveis para a Dynatrace, a Dynatrace tomará medidas comercialmente razoáveis para ajudar o Cliente no cumprimento de suas obrigações necessárias para permitir que o Cliente notifique Violações de Dados Pessoais relevantes às autoridades competentes e/ou Dados afetados, sujeito, se o Cliente for obrigado a fazê-lo de acordo com a Lei de Proteção de Dados aplicável. A notificação de uma violação de dados pessoais será entregue a um ou mais administradores do Cliente por qualquer meio selecionado pela Dynatrace, inclusive por e-mail. É responsabilidade exclusiva do Cliente garantir que os administradores do Cliente mantenham informações de contato precisas no portal on-line ou conforme exigido pela Dynatrace em um aviso por escrito ao(s) administrador(es) do Cliente. A obrigação da Dynatrace de relatar ou responder a uma Violação de Dados Pessoais nos termos desta Seção não é um reconhecimento por parte da Dynatrace de qualquer falha ou responsabilidade com relação à Violação de Dados Pessoais.

10. Subprocessamento

(a) O Cliente dá sua autorização geral para nomear membros do Grupo Dynatrace como subprocessadores nos termos deste CPD e autoriza a Dynatrace e os membros do Grupo Dynatrace a contratar outros Subprocessadores. Uma lista atualizada dos Subprocessadores atuais para as Ofertas da Dynatrace está disponível em https://www.dynatrace.com/company/trust-center/customers/subprocessors-dynatrace-services/ Para ser notificado sobre novos Subprocessadores ou alterações em Subprocessadores, o Cliente deve registrar-se para receber notificações disponíveis em https://www.dynatrace.com/company/trust-center/customers/subprocessors-dynatrace-services/ ("**Notificação de Proteção de Dados**"). A Dynatrace atualizará a Lista de Subprocessadores para refletir qualquer adição ou alteração em Subprocessadores terceirizados pelo menos trinta (30) dias antes da data efetiva da alteração. Os clientes que se inscreveram para receber atualizações da Lista de Subprocessadores serão notificados sobre a alteração.

(b) Na medida exigida pela Lei de Proteção de Dados aplicável, o Cliente poderá se opor ao processamento dos Dados Pessoais do Cliente por qualquer Subprocessador recém-nomeado por motivos razoáveis relacionados à proteção dos Dados Pessoais do Cliente e deverá informar a Dynatrace por escrito no prazo de quinze (15) dias após a notificação das alterações ser publicada na Lista de Subprocessadores, estabelecendo os motivos específicos para sua objeção. A objeção do Cliente deve ser feita por escrito e fornecer uma justificativa comercialmente razoável para a objeção, com base em preocupações razoáveis relativas às práticas do Subprocessador proposto relacionadas à proteção de dados. Após uma objeção, as partes trabalharão juntas de boa fé para abordar as objeções razoáveis do Cliente e prosseguir com a mudança no Subprocessador. Se um acordo não puder ser alcançado dentro de quinze (15) dias após a objeção, a critério da Dynatrace: (a) a Dynatrace instruirá o Subprocessador a não processar os Dados Pessoais do Cliente, o que pode resultar na suspensão e indisponibilidade de um recurso das Ofertas da Dynatrace. O Cliente, ou (b) o Cliente poderá rescindir imediatamente este CPD e o Contrato e a Dynatrace reembolsará imediatamente uma parte proporcional de quaisquer taxas pré-pagas para o período após tal suspensão ou data de rescisão. Se nenhuma objeção for recebida pela Dynatrace dentro do prazo especificado acima, considerar-se-á que o Cliente aprovou o uso do novo subprocessador.

(c) A Dynatrace deverá: (i) celebrar um acordo por escrito com cada Subprocessador contendo obrigações de

proteção de dados que forneçam obrigações contratuais apropriadas substancialmente semelhantes, mas não menos restritivas do que aquelas estabelecidas neste CPD, na medida apropriada à natureza do o serviço prestado por tal Subprocessador; e (ii) permanecerá responsável pelo cumprimento de tal Subprocessador com as obrigações deste CPD e por quaisquer atos ou omissões de tal Subprocessador que façam com que a Dynatrace viole qualquer uma de suas obrigações sob este CPD.

11. **Exclusão de Dados do Cliente em Rescisão**. Após a rescisão ou expiração do Contrato, os Dados Pessoais do Cliente serão excluídos dentro de trinta (30) dias ou, à escolha do cliente, devolvidos, exceto conforme exigido pela lei aplicável ou na medida em que sejam arquivados em sistemas de backup, e nesse caso, os termos deste CPD sobreviverão

12. **Transferências Internacionais de Dados**

(a) O Cliente autoriza a Dynatrace e seus Subprocessadores a transferir Dados Pessoais do Cliente através de fronteiras internacionais, incluindo, sem limitação, do EEA, Reino Unido e/ou Suíça, Israel e China para os Estados Unidos. Se os Dados Pessoais do Cliente originários do EEA ou da Suíça forem transferidos para um país que não oferece um nível adequado de proteção sob a Lei de Proteção de Dados aplicável ("**Transferência Restrita**"), as partes concordam que a transferência será regida pelas Cláusulas Contratuais Padrão que são incorporadas por referência neste CPD como segue. As assinaturas neste CPD ou no Contrato constituem a assinatura das Cláusulas Contratuais Padrão e de quaisquer anexos a elas anexados. Quando a transferência de Dados Pessoais do Cliente ("**Exportador de Dados**") para a Dynatrace ("**Importador de Dados**") for uma Transferência Restrita e as Leis de Proteção de Dados exigirem que um mecanismo de transferência válido seja implementado, as transferências estarão sujeitas ao Padrão Cláusulas Contratuais.

(b) As Cláusulas Contratuais Padrão serão preenchidas da seguinte forma:

i. O Módulo Dois será aplicado (conforme descrito);

ii. Na Cláusula 7 (Encaixe), será aplicada a cláusula de encaixe facultativo;

iii. Na Cláusula 8.5 e na Cláusula 16 (d), a certificação de exclusão será fornecida mediante solicitação por escrito do exportador de dados;

iv. Na Cláusula 8.9, o direito de auditoria será realizado de acordo com a Seção 7 do CPD;

v. Na Cláusula 9 (Uso de Subprocessadores), a opção 2 "Autorização Geral por Escrito" para subprocessadores será aplicada e o prazo para notificação prévia será o estabelecido na seção 11 deste CPD;

vi. Na Cláusula 11 (Reparação), a redação facultativa não se aplica;

vii. Na cláusula 13 (Supervisão), a autoridade de supervisão competente será a Commission Nationale de l'informatique et des libertes (CNIL).

viii. Na Cláusula 14 (f) e na Cláusula 16 (c), o direito de rescisão estará limitado à extinção das Cláusulas;

ix. Na Cláusula 17 (Lei Aplicável), as Cláusulas Contratuais Padrão serão regidas pela lei Francesa;

x. Na Cláusula 18(b) (Escolha do Foro e da Jurisdição), as partes concordam que as disputas serão resolvidas perante os tribunais da França;

xi. O Anexo 1 das Cláusulas Contratuais Padrão deverá ser preenchido com as informações constantes do Anexo A deste CPD;

xii. O Anexo 2 das Cláusulas Contratuais Padrão deverá ser preenchido com as informações constantes do Anexo B deste CPD; e

xiii. Uma nova Cláusula 1 (e) é adicionada às Cláusulas Contratuais Padrão, que deve ser lida: "Na medida aplicável neste documento, estas Cláusulas também se aplicam *"mutatis mutandis"* ao Processamento de Dados Pessoais do Cliente pelas partes que está sujeito à Lei Federal Suíça sobre Dados Proteção. Quando aplicável, a referência à legislação do Estado-Membro da UE ou às autoridades de supervisão

da UE será modificada para incluir a referência apropriada ao abrigo da legislação suíça no que se refere à transferência de Dados Pessoais do Cliente que estão sujeitos à Lei Federal Suíça sobre Proteção de Dados e à Lei Federal Suíça de Proteção de Dados. Comissário de Proteção e Informação como autoridade supervisora sob estas Cláusulas."

(c) Na medida em que o fornecimento das Ofertas da Dynatrace pela Dynatrace envolva a transferência de Dados Pessoais do Cliente originados do Reino Unido para um terceiro país que não tenha sido designado como fornecendo um nível adequado de proteção para Dados Pessoais do Cliente sob as Leis Aplicáveis no Reino Unido , as Cláusulas Contratuais Padrão deverão: (i) ser utilizadas e preenchidas conforme estabelecido na seção 13; (ii) uma nova Cláusula 1(f) é adicionada às Cláusulas Contratuais Padrão, que deve ser lida: "Na medida aplicável aqui, estas Cláusulas, conforme complementadas pela Seção 13, também se aplicam mutatis mutandis ao Processamento de Dados Pessoais do Cliente pelas partes que esteja sujeito às Leis de Proteção de Dados do Reino Unido; e (iii) o Adendo do Reino Unido será preenchido da seguinte forma:

i. A Tabela 1 do Adendo do Reino Unido deve ser preenchida com as informações do Anexo A.

ii. A Tabela 2 do Adendo do Reino Unido deverá ser preenchida com as informações localizadas na Seção 13 (c) deste CPD.

iii. A Tabela 3 do Adendo do Reino Unido deve ser preenchida da seguinte forma:

1) A lista das partes consta do Anexo A;

2) A Uma descrição da transferência está estabelecida no Anexo A;

3) A descrição das medidas técnicas e organizacionais constam do Anexo B;

4) A lista de subprocessadores consta na seção 11 deste CPD;

5) Para efeitos de preenchimento da Tabela 4 do Adendo do Reino Unido, tanto o importador como o exportador podem rescindir o Adendo do Reino Unido, conforme estabelecido na Secção 19 do Adendo do Reino Unido.

(d) Na medida em que o fornecimento das Ofertas da Dynatrace pela Dynatrace envolva a transferência de Dados Pessoais do Cliente originados da China para um terceiro país que não tenha sido designado como fornecendo um nível adequado de proteção para Dados Pessoais do Cliente sob as Leis Aplicáveis na China), O Cliente será responsável por cumprir todas as seguintes obrigações de exportação de Dados Pessoais do Cliente (onde o Cliente é o Controlador) ou garantir que todas as seguintes obrigações foram cumpridas pelo controlador terceirizado relevante (onde o Cliente é o Processador):

i. informar aos indivíduos o nome e as informações de contato da parte receptora dos Dados Pessoais do Cliente no exterior, a finalidade e os meios do Processamento, as categorias de Dados Pessoais do Cliente e os métodos e procedimentos por meio dos quais os indivíduos podem fazer solicitações para exercer os direitos aos Dados Pessoais do Cliente com a parte receptora dos Dados Pessoais do Cliente no exterior;

ii. garantir uma base legal para a exportação de Dados Pessoais do Cliente e, quando o consentimento dos indivíduos for a base legal, obter o consentimento separado dos indivíduos;

iii. realizar uma avaliação de impacto da proteção de informações pessoais na exportação de Dados Pessoais do Cliente; e

iv. adotar a medida de salvaguarda apropriada exigida pelo PIPL e regulamentos administrativos que a acompanham (ou seja, passar na avaliação de segurança do governo, preencher as cláusulas contratuais padrão executadas ou obter a certificação), a menos que se aplique isenção.

(e) Adicionalmente acima exposto, se uma Autoridade Supervisora adotar, atualizar ou substituir quaisquer cláusulas contratuais padrão ou mecanismos semelhantes de transferência de dados, a Dynatrace reserva-se o direito de adotar um padrão de conformidade alternativo para substituir ou complementar as Cláusulas Contratuais Padrão ou o Adendo do Reino Unido para a transferência legal de Dados Pessoais, ou adicionar

novos mecanismos de transferência de dados para outros países, desde que sejam reconhecidos pela Lei de Proteção de Dados. A Dynatrace fornecerá um aviso com 30 (trinta) dias de antecedência sobre a adoção do padrão de conformidade alternativo aos clientes que assinarem os Avisos de Proteção de Dados. A alteração será aplicada automaticamente conforme estabelecido na notificação da Dynatrace no final do período de aviso prévio.

(f) No caso de qualquer conflito ou inconsistência entre os seguintes documentos, a ordem de precedência será: (1) as Cláusulas Contratuais Padrão (desde que, no entanto, o Operador possa nomear Subprocessadores conforme estabelecido e sujeito aos requisitos da Seção 11 deste CPD) ou um mecanismo semelhante exigido pelas Leis de Proteção de Dados aplicáveis especificamente para transferências internacionais de dados; (2) este CPD; e (3) o Acordo.

(g) Na medida em que a Dynatrace transfere Dados do Cliente originados e protegidos pela Lei de Proteção de Dados aplicável no Brasil, a Dynatrace deverá cumprir os princípios e direitos dos Titulares dos Dados e as obrigações de proteção de dados previstas na LGPD.

(h) Na medida em que a Dynatrace transfere Dados do Cliente originados e protegidos pela Lei de Proteção de Dados aplicável no Japão, a Dynatrace deverá cumprir os princípios e direitos dos Titulares dos Dados e as obrigações de proteção de dados previstas na APPI.

(i) Na medida em que o fornecimento das Ofertas da Dynatrace pela Dynatrace envolva a transferência de Dados Pessoais do Cliente originados de Israel para um país terceiro que não tenha sido designado como fornecendo um nível adequado de proteção para os Dados Pessoais do Cliente de acordo com as Leis Aplicáveis em Israel), o Cliente será responsável por garantir uma base legal para a exportação de Dados Pessoais do Cliente. Para maior clareza, este CPD constitui uma obrigação por escrito da Dynatrace para adotar as medidas de proteção apropriadas exigidas pelos Regulamentos de Proteção de Privacidade (Transferência Internacional de Dados) de 2001. Por uma questão de clareza, as obrigações deste CPD são consideradas suficientes pelo Cliente para facilitar a transferência de informações para fora de Israel, de acordo com o Regulamento 3 dos Regulamentos de Proteção de Privacidade (Transferência de Dados para Bancos de Dados Fora das Fronteiras do País), 2001.

13.Termos Específicos das Leis de Privacidade Estaduais Suplementares dos EUA.

(a) A definição de “Lei de Proteção de Dados Aplicável” inclui as Leis de Leis de Privacidade Estaduais dos EUA. “Leis Estaduais de Privacidade dos EUA” significa todas as leis estaduais relacionadas à proteção e processamento de dados pessoais em vigor nos Estados Unidos da América, que podem incluir, sem limitação, a Lei de Privacidade do Consumidor da Califórnia, conforme alterada pela Lei de Direitos de Privacidade da Califórnia (“CCPA”) e leis semelhantes de privacidade do consumidor em outros estados, em cada caso, conforme alteradas, complementadas ou substituídas de tempos em tempos.

(b) Quando a Dynatrace processa Dados Pessoais do Cliente, estes estão sujeitos às Leis de Privacidade Estaduais dos EUA, a Dynatrace é um “provedor de serviços” ou “processador” (conforme aplicável) ao processar dados Pessoais do Cliente. O Cliente divulga, ou de outra forma disponibiliza, Dados Pessoais do Cliente à Dynatrace para uma finalidade limitada e específica de fornecer Ofertas da Dynatrace de acordo com o Contrato (o “Objeto”). A Dynatrace deverá (e exigirá que seus Subprocessadores):

i. cumprir as obrigações que lhe são aplicáveis enquanto provedor de serviços ou processador sujeitos às Leis de Privacidade Estaduais dos EUA;

ii. notificar se não puder mais cumprir suas obrigações perante as Leis de Privacidade Estaduais dos EUA;

iii. não “vender” ou “compartilhar” (conforme tais termos definidos pela CCPA) Conteúdo do Cliente ou reter, usar ou divulgar Dados Pessoais do Cliente: (1) para qualquer finalidade diferente da Finalidade, incluindo reter, usar ou divulgar Dados Pessoais do Cliente para uma finalidade comercial diferente da Finalidade, ou conforme permitido pelas Leis de Privacidade Estaduais dos

EUA; ou (2) fora do relacionamento comercial direto entre o Cliente e a Dynatrace; ou, a menos que permitido de outra forma pelas Leis de Privacidade Estaduais dos EUA, não combinar Dados Pessoais do Cliente com Dados Pessoais que a Dynatrace recebe de ou em nome de outra empresa ou pessoa, ou que coleta de suas próprias interações com indivíduos, a menos que tal combinação seja necessária para realizar qualquer finalidade comercial, conforme permitido pelas Leis de Privacidade Estaduais dos EUA.

iv. O Cliente: (1) mediante notificação, terá o direito de tomar medidas razoáveis e apropriadas acordadas pelas partes para ajudar a garantir que a Dynatrace Processe os Dados Pessoais do Cliente de maneira consistente com as obrigações do Cliente sob a Leis de Privacidade Estaduais dos EUA e para interromper e remediar o Processamento não autorizado de Dados Pessoais do Cliente pela Dynatrace Processamento de Dados Pessoais do Cliente pela Dynatrace; (2) notificar o Cliente se determinar que não pode mais cumprir suas obrigações de acordo com a Leis de Privacidade Estaduais dos EUA em relação Dados Pessoais do Cliente.

v. A Dynatrace reconhece e confirma que não recebe Dados Pessoais do Cliente como contraprestação por quaisquer Ofertas fornecidas ao Cliente. A Dynatrace certifica que entende e cumprirá suas obrigações sob a Leis de Privacidade Estaduais dos EUA

5 Demais condições

(a) Exceto conforme alterado por este CPD, o Contrato permanecerá em pleno vigor e efeito. Quaisquer alterações a este CPD devem ser feitas por escrito e devidamente assinadas por representantes autorizados das partes.

(b) Não obstante qualquer disposição em contrário no Contrato ou neste CPD, a responsabilidade de cada parte e de todas as suas Afiliadas, tomadas em conjunto, decorrentes ou relacionadas a este CPD, qualquer pedido ou Contrato, seja em contrato, ato ilícito ou sob qualquer outra teoria de responsabilidade, permanecerá sujeita à seção "Limitação de Responsabilidade" do Contrato, e qualquer referência em tal seção à responsabilidade de uma parte significa a responsabilidade agregada dessa parte e de todas as suas Afiliadas sob o Contrato e este CPD, incluindo todos os Anexos deste instrumento. A Dynatrace não será responsável perante o Cliente por perdas ou danos indiretos ou consequentes, perda de lucros, perda de vendas, perda de negócios, perda de economias antecipadas, perda ou dano à boa vontade ou, de outra forma, em cada caso, direta ou indireta, que surja de ou em conexão com este CPD. Sem limitar as obrigações de qualquer uma das partes nos termos do Contrato ou deste CPD, o Cliente concorda que qualquer responsabilidade incorrida pela Dynatrace em relação aos Dados Pessoais do Cliente que surja como resultado de, ou em conexão com, o não cumprimento pelo Cliente de suas obrigações sob este CPD ou a Lei de Proteção de Dados aplicável contará e reduzirá o limite de responsabilidade da Dynatrace nos termos do Contrato (ou, se aplicável, sob este CPD) como se fosse responsabilidade para com o Cliente. Não obstante qualquer disposição em contrário neste CPD (incluindo, sem limitação, as obrigações de indenização de qualquer uma das partes), nenhuma das partes será responsável por quaisquer multas do GDPR emitidas ou cobradas nos termos do Artigo 83 do GDPR contra a outra parte por uma autoridade reguladora ou órgão governamental em conexão com a violação do GDPR por essa outra parte.

(c) Este CPD será regido e interpretado de acordo com a lei aplicável e as disposições de jurisdição do Contrato, desde que as Cláusulas Contratuais Padrão sejam regidas conforme estabelecido na seção 13 deste CPD.

Assinado por e em nome do **CLIENTE:**	Assinado por e em nome da **DYNATRACE**
Assinatura	Assinatura
Nome	Nome
Cargo	Cargo

Data	Data

ANEXO A
DETALHES DO PROCESSAMENTO

Descrição da Exportação de Dados

O exportador de dados é a entidade identificada como o "Cliente" ou "Dynatrace", conforme o caso no caso de qualquer Subprocessamento, no Contrato de Processamento de Dados em vigor entre o exportador e o importador de dados e ao qual este Anexo está anexado.

Descrição da Importação de Dados

O importador de dados é a entidade identificada como "Dynatrace" ou um Subprocessador devidamente autorizado no Contrato de Processamento de Dados em vigor entre o exportador e o importador de dados e ao qual este cronograma é anexado.

Objeto e Duração do Processamento

O objeto e a duração do processamento são os seguintes:

Entre as partes, o Cliente será o Controlador de determinados Dados Pessoais do Cliente fornecidos à Dynatrace pelo Cliente em conexão com o uso das Ofertas da Dynatrace. A duração do processamento será a vigência do Contrato.

Finalidades do Tratamento

O processamento é necessário para os seguintes fins:

Para permitir que a Dynatrace forneça suas Ofertas ao Cliente e exerça seus direitos e obrigações nos termos do Contrato.

Titulares dos Dados

Os titulares dos dados podem incluir: (i) usuários autorizados pelo Cliente a usar as Ofertas da Dynatrace e (ii) usuários ou visitantes dos aplicativos e/ou sites monitorados do Cliente (incluindo, entre outros, funcionários, clientes ou clientes, agentes, contratados e consultores do Cliente), conforme determinado a critério exclusivo do Cliente.

Tipo de Dados Pessoais

O Cliente é obrigado a fornecer determinados Dados Pessoais para usar as Ofertas da Dynatrace, incluindo endereço IP e nome e sobrenome, se incluídos no endereço de e-mail e nas credenciais do usuário de um usuário. O Cliente pode enviar Dados Pessoais adicionais para as Ofertas da Dynatrace, cuja extensão é determinada e controlada pelo Cliente a seu exclusivo critério

Categorias Especiais de Dados ou Dados Pessoais Sensíveis (se apropriado)

Os Dados Pessoais transferidos dizem respeito às seguintes categorias especiais de dados ou dados pessoais sensíveis:

Não aplicável. O Cliente não pode usar as Ofertas da Dynatrace para processar quaisquer dados classificados como "dados de categoria especial" ou "dados pessoais confidenciais", a menos que explicitamente acordado por escrito

Operações do Processamento

Os dados pessoais transferidos estarão sujeitos às seguintes atividades básicas de processamento:

A Dynatrace processará os Dados Pessoais do Cliente somente conforme necessário para fornecer as

Ofertas da Dynatrace e exercer seus direitos e obrigações conforme contidos nos termos do Contrato e deste Contrato de Processamento de Dados, incluindo, entre outros, capacitação do cliente, suporte técnico, serviços profissionais, melhoria do desempenho e das funções das Ofertas da Dynatrace, autenticação e comunicações do usuário e administração da conta.

ANEXO B

MEDIDAS DE SEGURANCA

A Dynatrace (também referida neste documento como "Processador") implementará, pelo menos, as medidas de segurança técnicas e organizacionais descritas abaixo em relação aos Dados Pessoais do Cliente que processa em nome do Cliente (também referido aqui como "Controlador"). Essas medidas de segurança devem ser aplicadas a todos os Dados Pessoais do Cliente que estão sujeitos ao contrato subjacente entre o Processador e o Controlador (o "Contrato"). Em relação a subprocessadores terceirizados que podem processar Dados Pessoais em nome da Dynatrace, esses terceiros terão seus próprios requisitos de segurança para proteger os Dados Pessoais .

Medidas Técnicas

1.1 Autorização

(a) Deverá ser utilizado um sistema de autorização quando forem utilizados diferentes perfis de autorização para diferentes fins.

1.2 Identificação

(a) Cada Usuário Autorizado deve receber um código de identificação pessoal e exclusivo para esse fim ("ID de Usuário"). Um ID de usuário não pode ser atribuído a outra pessoa, mesmo em um momento subsequente.

(b) Deve ser mantido um registro atualizado dos Usuários Autorizados, e o acesso autorizado disponível para cada um, e procedimentos de identificação e autenticação devem ser estabelecidos para todo acesso a sistemas de informação ou para a realização de qualquer Tratamento de Dados. Conforme usado neste documento, "Processamento" refere-se a qualquer operação ou conjunto de operações realizadas nos Dados, seja ou não por meios automatizados, como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou disponibilização, alinhamento ou combinação, restrição, apagamento ou destruição.

(c) As senhas devem ser modificadas periodicamente, conforme estabelecido nas Políticas de Segurança da Informação.

1.3 Autenticação

(a) Os Usuários Autorizados terão permissão para Processar Dados se receberem credenciais de autenticação, de modo a concluir com êxito um procedimento de autenticação relacionado a uma operação de Processamento específica ou a um conjunto de operações de Processamento.

(b) A autenticação deve ser baseada em uma senha secreta associada ao ID do usuário, e essa senha deve ser conhecida apenas pelo usuário autorizado.

(c) Uma ou mais credenciais de autenticação devem ser atribuídas ou associadas a um Usuário Autorizado.

(d) Deve haver um procedimento para confidencialidade e integridade da senha. As senhas devem ser armazenadas de forma a torná-las ininteligíveis enquanto permanecerem válidas. Deve haver um procedimento para atribuir, distribuir e armazenar senhas.

(e) As senhas devem ser compostas, pelo menos, por doze caracteres ou, se tal não for tecnicamente permitido pelos sistemas de informação pertinentes, uma palavra-passe deve ser constituída pelo número máximo permitido de caracteres. As senhas não devem conter nenhum item que possa ser facilmente relacionado ao Usuário Autorizado responsável pelo Tratamento e devem ser alteradas em intervalos regulares, intervalos esses que devem ser estabelecidos no documento de segurança. As senhas devem ser modificadas pelo Usuário Autorizado para um valor secreto conhecido apenas pelo Usuário Autorizado quando for usado pela primeira vez e periodicamente depois disso.

(f) Além de uma combinação válida de identificação de usuário e senha, todo o acesso aos dados ou sistemas da Dynatrace deve ser protegido por uma solução de autenticação multifator ("MFA"). A solução MFA pode ser de natureza de software ou hardware.

(g) As credenciais de autenticação também serão desativadas se o Usuário Autorizado for encerrado, transferido ou desautorizado de acessar os sistemas de informação ou Dados de Processamento.

1.4 Controle de Acesso

(a) Somente Usuários Autorizados terão acesso aos Dados, inclusive quando armazenados em qualquer mídia eletrônica ou portátil ou quando transmitidos. Os Usuários Autorizados terão acesso autorizado apenas aos dados e recursos necessários para o desempenho de suas funções.

(b) Deve ser utilizado um sistema para conceder aos Usuários Autorizados acesso aos dados e recursos designados.

(c) Deve ser verificado semestralmente se continuam a ser aplicáveis as condições prévias para a manutenção dos perfis de autorização correspondentes. Isso também pode incluir a lista de Usuários Autorizados elaborada por categorias homogêneas de tarefas e perfil de autorização correspondente.

(d) Devem ser tomadas medidas para impedir que um usuário obtenha acesso ou utilização não autorizados dos sistemas de informação. Em particular, sistemas de detecção de intrusão que reflitam as melhores práticas do setor devem ser instalados para proteger os sistemas de informação contra acesso não autorizado

(e) Os controles de acesso ao sistema operacional ou ao banco de dados devem ser configurados corretamente para garantir apenas o acesso autorizado.

(f) Somente pessoas autorizadas pode conceder, alterar ou cancelar o acesso dos usuários aos sistemas de informação.

1.5 Gerenciamento de sistemas de computadores e mídias removíveis

(a) Os sistemas de informação de rede e o armazenamento de Dados físicos devem ser alojados em um ambiente seguro, com acesso físico restrito à equipe autorizada a ter esse acesso. Controles fortes de autorização e acesso devem ser mantidos

(b) O software, firmware e hardware utilizados nos sistemas de informação devem ser revistos anualmente, a fim de detetar vulnerabilidades e falhas nos sistemas de informação e resolver tais vulnerabilidades e falhas

(c) Políticas e treinamentos devem ser emitidos com relação à manutenção e uso da mídia na qual os Dados são armazenados, a fim de impedir acessos e o Processamentos não autorizados.

(d) Quando os meios de comunicação forem eliminados ou reutilizados, devem ser tomadas as medidas necessárias para evitar qualquer recuperação posterior dos Dados e de outras informações anteriormente armazenadas nos mesmos, ou para tornar as informações inteligíveis ou reconstruídas por qualquer meio técnico antes de serem retiradas do inventário. Todas as mídias reutilizáveis usadas para o armazenamento de Dados serão substituídas no mínimo três vezes por dados aleatórios antes do descarte ou reutilização

(e) A remoção de mídia contendo Dados das instalações designadas deve ser especificamente autorizada pelo Controlador e em conformidade com as políticas da Dynatrace

(f) A mídia que contiver dados deve ser apagada ou tornada ilegível se não for mais usada e antes do descarte adequado.

1.6 Distribuição ou Transmissão

(a) Dados devem estar disponíveis apenas para usuários autorizados.

(b) A criptografia (128 bits ou mais forte) ou outra forma equivalente de proteção deve ser usada para proteger os Dados transmitidos eletronicamente por uma rede pública ou armazenados em um dispositivo portátil, ou quando houver um requisito para armazenar ou processar Dados em um ambiente fisicamente inseguro.

(c) Quando Dados saírem das instalações designadas como resultado de operações de manutenção, as medidas necessárias devem ser tomadas para evitar qualquer recuperação não autorizada dos Dados e outras informações neles armazenadas.

(d) Quando Dados são transmitidos ou transferidos através de uma rede de comunicações eletrônicas, devem ser implementadas medidas para controlar o fluxo de dados e registar o momento da transmissão ou transferência, os Dados transmitidos ou transferidos, o destino de quaisquer Dados transmitidos ou transferidos e os detalhes do Utilizador Autorizado que realiza a transmissão ou transferência.

1.7 Preservação, copias de Back-up (Copias de Segurança) e Recuperação

(a) Devem ser definidos e estabelecidos procedimentos para a realização de cópias de segurança e para a recuperação dos dados. Esses procedimentos devem prever que os Dados sejam reconstruídos no estado em que se encontravam no momento em que foram perdidos ou destruídos.

(b) As cópias de segurança devem ser feitas pelo menos uma vez por semana, a menos que nenhum dado tenha sido atualizado durante esse período.

(c) Uma cópia de segurança e os procedimentos de recuperação de dados devem ser mantidos em um local diferente do local dos sistemas de informação que processam os dados e esses requisitos mínimos de segurança devem ser aplicados a essas cópias de backup.

1.8 Antivírus e detecção de invasão

(a) O software antivírus e os sistemas de detecção de invasão devem ser instalados nos sistemas de informação para proteção contra-ataques ou outros atos não autorizados em relação aos sistemas de informação. O software antivírus e os sistemas de detecção de intrusão devem ser atualizados regularmente de acordo com as melhores práticas do setor para os sistemas de informação em questão (e pelo menos anualmente).

1.9 Testes

(a) O teste prévio à implementação ou modificação dos sistemas de informação de processamento de dados não devem usar dados reais ou "em produção", a menos que tal uso seja necessário e

não haja alternativa razoável. Quando forem utilizados dados reais ou "em produção", estes devem ser limitados ao necessário para efeitos de teste e deve ser garantido o nível de segurança correspondente ao tipo de Dados Tratados.

1.10 Auditoria

(a) Devem ser realizadas auditorias regulares do cumprimento destes requisitos de segurança, pelo menos uma vez por ano.

(b) Os resultados devem fornecer um parecer sobre a medida em que controles de segurança adotados cumpriram esses requisitos de segurança, identificar quaisquer deficiências e (se for caso disso) propor medidas corretivas ou suplementares, se necessário. Deve também incluir os dados, factos e observações sobre os quais os pareceres foram emitidos, bem como as recomendações propostas.

2. Medidas organizacionais

2.1 Plano e documento de segurança

- As medidas adotadas para cumprir estes requisitos de segurança serão objeto das Políticas de Segurança da Informação da Empresa e constarão no portal de segurança, que deverá ser mantido atualizado, e revisto sempre que sejam efetuadas alterações relevantes no(s) sistema(s) de informação ou em medidas técnicas ou organizativas.
- As Políticas de Segurança da Informação devem abordar:

  (i) Medidas de segurança relacionadas à modificação e manutenção do(s) sistema(s) usado(s) para processar dados, incluindo desenvolvimento e manutenção de aplicativos, suporte apropriado do fornecedor e um inventário de hardware e software;

  (ii) Segurança física, incluindo segurança dos edifícios ou instalações onde ocorre o Tratamento de Dados, segurança de equipamentos de dados e infraestrutura de telecomunicações e controles ambientais; e

  (iii) Segurança de computadores e sistemas de telecomunicações, incluindo procedimentos de gestão de cópias de segurança, procedimentos relativos a vírus informáticos, procedimentos de gestão de sinais/códigos, segurança da implementação de software, segurança relacionada com bases de dados, segurança da ligação de sistemas à Internet, Inspecção da evasão de sistemas de dados, mecanismos para ter em conta as tentativas de violação da segurança do sistema ou de obtenção de acesso não autorizado.

- O plano de segurança deve incluir todas as políticas da Dynatrace, atualizadas periodicamente, incluindo, mas não se limitando a:

  (i) Código de Ética e Conduta Empresarial;

  (ii) Política Global de Proteção de Dados;

  (iii) Aceitação da Política de IT da Dynatrace

  (iv) Políticas de Segurança do Sistema: Política de Gerenciamento de Controle de Acesso Dynatrace; Padrão de retenção de backup; Política de Gestão de Mudanças; Política de Gestão de Mudanças - Sistemas de Negócios; Política de Compliance; Plano de Resposta a Incidentes de Segurança Cibernética e de Dados; Política de Classificação de Dados; Política de Prevenção de Perda de Dados; Política de Monitoramento Eletrônico; Política de Criptografia; Política de Segurança de Recursos Humanos; Política de Gestão de Recursos de Informação; Política de Gestão de Riscos da Informação; Política de Operações de TI; Política de Dispositivos Móveis; Política de Acesso à Rede; Política de senha de conta de rede; Política de Firewall de Rede; Segurança Física e Política Ambiental; Política de Devolução de Ativos para Funcionários Demitidos; Seguro; Política de Phishing de Segurança; Política de Ciclo de Vida da Conta de Serviço; Política de Gestão de

Fornecedores; Política de Gestão de Vulnerabilidades; Política de segurança da estação de trabalho .

(v) O plano de segurança deve estar disponível para o pessoal que tenha acesso aos dados e aos sistemas de informação e deve abranger, no mínimo, os seguintes aspetos:

(vi) O escopo, com uma especificação detalhada dos recursos protegidos;

(vii) As medidas, normas, procedimentos, regras do código de conduta e normas para garantir a segurança, incluindo o controle, inspeção e supervisão dos sistemas de informação;

(viii) Os procedimentos para relatar, gerenciar e responder a incidentes; e

(ix) Os procedimentos para fazer cópias de segurança e recuperar Dados, incluindo o membro da equipe que realizou a atividade de Processamento, os Dados restaurados e, conforme apropriado, quais dados tiveram que ser inseridos manualmente no processo de recuperação.

2.2 Funções e obrigações das equipes responsáveis

- Somente os membros da equipe que tenham necessidade operacional legítima de acessar os sistemas de informação ou realizar qualquer Tratamento de Dados serão autorizados a fazê-lo ("**Usuários Autorizados**").
- Devem ser adotadas as medidas necessárias para formar e familiarizar a equipe com estes requisitos mínimos de segurança, quaisquer políticas relevantes e leis aplicáveis relativas ao desempenho das suas funções e deveres em relação ao Tratamento de Dados e as consequências de qualquer violação destes requisitos.
- As funções e obrigações do pessoal que possuem acesso aos Dados e aos sistemas de informação devem ser claramente definidas através de funções de segurança da aplicação.
- Os Usuários Autorizados devem ser instruídos no sentido de que qualquer equipamento eletrônico, não deve ser deixado sem supervisão ou acessível durante as sessões de Processamento. O acesso físico às áreas onde quaisquer Dados são armazenados deve ser restrito aos Usuários Autorizados. As medidas disciplinares em caso de infracção ao plano de segurança devem ser claramente definidas, documentadas e comunicadas ao pessoal.

2.3 Diretor de Segurança (Chief Security Officer)

- Uma pessoa ou pessoas responsáveis pela conformidade geral com esses requisitos mínimos de segurança devem ser designadas como "**Diretor de Segurança**" e/ou "Chief Information Security Officer ("**CISO**"). O **DS** ou **CISO** deve ter formação adequada e experiência na gestão da segurança da informação e dispor de recursos adequados para garantir eficazmente a conformidade.
- Os dados de contato do **DS** ou **CISO** devem ser fornecidos ao responsável pelo tratamento, mediante pedido.

2.4 Manutenção de Registros

- Um histórico de acesso ou divulgação de Dados do Usuário Autorizado deve ser registrado com uma trilha de auditoria segura.
- Somente a equipe devidamente autorizada pode ter acesso físico às instalações onde os sistemas de informação e a mídia que armazenam Dados são armazenados.
- Deve existir um procedimento para comunicar, responder e gerir incidentes de segurança, tais

como violações da segurança dos dados. Tal deve incluir, no mínimo, :

(i) Um procedimento para relatar tais incidentes/violações à administração apropriada;

(ii) Uma equipe claramente designada para gerenciar e coordenar a resposta a um incidente liderada pelo DS/CISO;

(iii) Um processo documentado para gerenciar a resposta a um incidente, incluindo a exigência de manter problemas apropriados e registros de ação para incluir a hora em que o incidente ocorreu, a pessoa que relatou o incidente, a quem foi relatado e seus efeitos;

(iv) A exigência de que o Processador notifique o Controlador sem demora injustificada se houver uma violação de segurança que leve à destruição, perda, alteração, divulgação ou acesso não autorizado acidental ou ilegal aos Dados transmitidos, armazenados ou processados de outra forma pelo Processador;

(v) A equipe de gerenciamento de segurança/incidentes do Processador deve, quando apropriado, trabalhar em conjunto com os representantes de segurança do Controlador até que o incidente ou violação seja resolvido satisfatoriamente; e

(vi) O procedimento de comunicação, gestão e resposta a incidentes deve ser testado pelo menos uma vez por ano.