

ACORDO DE PROCESSAMENTO DE DADOS DA PIX4D

Última modificação: Outubro de 2021

Este Acordo de Processamento de Dados e seus Anexos (juntos, o "DPA") são um acordo entre Você e a Pix4D (Pix4D e Você, cada um uma "Parte" e, coletivamente, as "Partes"), que rege o processamento de Dados do Pessoal do Cliente pela Pix4D em Seu nome em relação ao Acordo de Licença do Usuário Final (o "EULA"). Esse DPA é incorporado e faz parte do EULA.

A Pix4D pode atualizar este DPA de tempos em tempos. A versão disponível em nosso Site pix4d.com/legal é a versão atual.

Todos os termos que começam com letra maiúscula não definidos neste DPA têm os significados estabelecidos no EULA. Para evitar dúvidas, todas as referências ao EULA incluem este DPA (incluindo seus Anexos e o SCC da UE, conforme definido aqui) e, na medida aplicável, os Termos e Condições Gerais para Clientes da Pix4D (os "Termos Gerais") e qualquer termo adicional anexado aos mesmos que possam se aplicar em relação ao Uso de uma Oferta específica (os "Termos adicionais").

SUMÁRIO

CONSIDERANDO QUE	2
1. INÍCIO E DURAÇÃO	2
2. ESCOPO DA LEI DE PROTEÇÃO DE DADOS	2
3. PROCESSAMENTO DE DADOS E FUNÇÕES DAS PARTES	2
4. SOLICITAÇÕES DO SUJEITO DOS DADOS	4
5. PESSOAL DA PIX4D	4
6. SUBPROCESSADORES	4
7. SEGURANÇA DOS DADOS	5
8. TRANSFERÊNCIAS DE DADOS PARA PAÍSES NÃO NA LISTA DE PERMITIDOS	5
9. VIOLAÇÕES DE DADOS	7
10. SOLICITAÇÕES DE ACESSO A DADOS POR PARTE DO GOVERNO	7
11. REVISÃO E AUDITORIA DE CONFORMIDADE	7
12. AVALIAÇÕES DE IMPACTO E CONSULTORIAS	7
13. DEVOLUÇÃO OU EXCLUSÃO DE DADOS	7
14. LIMITAÇÃO DE RESPONSABILIDADE	8
15. DIVERSOS	8
16. LEI VIGENTE – RESOLUÇÃO DE DISPUTA	8
17. DETERMINAÇÕES ADICIONAIS PARA INFORMAÇÕES PESSOAIS NA CALIFÓRNIA 9	
18. DEFINIÇÕES	9

CONSIDERANDO QUE

- A. As Partes firmaram o EULA sob os Termos Gerais e os Termos Adicionais, conforme aplicável.
- B. No contexto da realização do EULA, a Pix4D e/ou qualquer de suas Afiliadas pode ter acesso a Dados Pessoais do Cliente divulgados ou de outra forma disponibilizados por meio das Ofertas Licenciadas sob o EULA por Você (ou a Seu critério) ou pelos Usuários Autorizados.
- C. Na medida em que a Pix4D processará esses Dados Pessoais do Cliente como Seu processador, as Partes desejam garantir que esse processamento esteja em conformidade com as Leis de Proteção de Dados aplicáveis e concordam com determinados termos e condições aplicáveis a tal processamento conforme estabelecido neste DPA.

Agora, portanto, as Partes concordam com o seguinte:

1. INÍCIO E DURAÇÃO

- 1.1. **Início.** Este DPA entrará em vigor e substituirá qualquer acordo de processamento de dados aplicável anteriormente a partir da Data Efetiva dos Termos (conforme definido abaixo).
- 1.2. **Duração.** Independentemente de o EULA ter terminado ou expirado, este DPA (incluindo as Cláusulas P-C conforme aplicável) continuará em vigor até, e expirará automaticamente quando, a Pix4D excluir todos os Dados do Cliente descritos neste DPA.

2. ESCOPO DA LEI DE PROTEÇÃO DE DADOS

- 2.1. **Aplicação das Leis de Proteção de Dados.** As Partes reconhecem que a Lei de Proteção de Dados Europeia e, conforme o caso, Proteção de Dados Não Europeia, se aplicará ao processamento de Dados pessoais do Cliente pela Pix4D.
- 2.2. **Aplicação das Determinações deste DPA.** Este DPA foi elaborado especificamente para os fins da Lei de Proteção de Dados Europeia, mas leva em conta também, na medida possível, os requisitos da Proteção de Dados Não Europeia, em particular, o CCPA conforme estabelecido na Seção 17, na medida aplicável. A menos que especificado de outra forma neste DPA, as determinações deste DPA serão aplicadas independentemente de a Lei de Proteção de Dados Europeia ou a Lei de Proteção de Dados Não Europeia se aplicar ao processamento de Dados Pessoais do Cliente.

3. PROCESSAMENTO DE DADOS E FUNÇÕES DAS PARTES

- 3.1. **Funções das Partes.** Na medida em que a Lei de Proteção de Dados Europeia se aplica, as Partes reconhecem e concordam que, com relação ao processamento de Dados Pessoais do Cliente no contexto da execução do EULA referente (i) aos Usuários Autorizados das Ofertas Licenciadas para os quais Você gerencia as Contas (e, em particular, decide quem tem acesso a uma Organização e em que medida) e/ou (ii) qualquer outro terceiro que apareça no Conteúdo divulgado ou de outra forma disponibilizado à Pix4D por meio das Ofertas Licenciadas sob o EULA, Você é o controlador e a Pix4D é o processador agindo em Seu nome.
- 3.2. **Processamento adicional pela Pix4D.** Não obstante a Seção 3.1 acima, você concorda que a Pix4D pode processar Dados Pessoais além de sua função de processador, ou seja, como controlador, para seus próprios fins nos seguintes

casos:

- (a) Com relação a Dados Pessoais de Usuários Autorizados das Ofertas Licenciadas, incluindo dados de uso, na medida necessária para operar as Ofertas Licenciadas (por exemplo, para fins de faturamento) e de outra forma realizar o EULA ou exercer seus direitos; especificamente, para dados de uso, desde que (a) tal uso seja para fins estatísticos, analíticos e outros não relacionados a pessoas específicas; e (b) qualquer informação, se houver, disponibilizada a terceiros (que não os prestadores de serviço da Pix4D sob obrigação de confidencialidade) (i) não contenha dados de identificação pessoal de Usuários Autorizados; e (ii) não contenha nenhum dado de identificação pessoal sobre Você; quando (a) e (b) não se aplicarem, processaremos dados de uso não anonimizados para fins de análise de uso e melhoria do produto na medida em que você tiver concordado com esse processamento nas configurações de privacidade da sua Conta pessoal.
- (b) Com relação a Dados Pessoais de terceiros que aparecem no Conteúdo divulgado ou de outra forma disponibilizado à Pix4D por meio da Oferta Licenciada, para seus próprios fins como controlador, desde que (a) tal uso seja para fins estatísticos, de pesquisa e desenvolvimento, de análise comparativa e outros não relacionados a pessoas específicas; e (b) qualquer informação, se houver, disponibilizada a terceiros (que não os prestadores de serviço da Pix4D sob obrigação de confidencialidade) não (i) contenham dados de identificação pessoal de terceiros; e (ii) não contenham nenhum dado de identificação pessoal sobre Você;
- (c) Em qualquer caso, para qualquer outro fim exigido ou permitido pelas Leis de Proteção de Dados e outras leis vigentes.

3.3. **Sua Conformidade e Instruções à Pix4D.** Você declara e garante que (i) Você cumpriu e continuará cumprindo todas as leis vigentes, incluindo Leis de Proteção de Dados, em relação ao Seu processamento de Dados Pessoais do Cliente, sua delegação à Pix4D e quaisquer instruções de processamento que Você emita à Pix4D; e (ii) Você forneceu e continuará fornecendo todos os avisos e obteve e continuará obtendo todos os consentimentos e direitos necessários sob as Leis de Proteção de Dados para a Pix4D processar Dados Pessoais do Cliente para os fins descritos no EULA. Você será o único responsável pela precisão, pela qualidade e pela legalidade dos Dados Pessoais do Cliente e os meios pelos quais Você adquiriu os Dados Pessoais do Cliente. Sem prejuízo à generalidade do precedente, Você concorda que Você será responsável por cumprir todas as leis (incluindo as Leis de Proteção de Dados) aplicáveis a qualquer Conteúdo criado, enviado ou gerenciado por meio das Ofertas Licenciadas sob o EULA. Você, por meio deste, autoriza e instrui a Pix4D a, ela própria, gerenciar e processar solicitações de exclusão de Conta do usuário em Seu nome na medida em que (i) tais solicitações sejam enviadas pelo Usuário diretamente à Pix4D pelo e-mail data_protection@pix4d.com ou outros meios e (ii) o Usuário seja um de Seus Usuários Autorizados. Nesse caso, a Pix4D poderá notificá-lo da solicitação de exclusão da conta na medida em que considerar necessário. O EULA (incluindo este DPA), junto com o Uso e o modo como Você configurou os Produtos Licenciados de acordo com o EULA, constitui Suas instruções completas à Pix4D em relação ao processamento relevante de Dados Pessoais do Cliente, enquanto você puder fornecer instruções adicionais durante o Prazo que sejam consistentes com o EULA, a natureza, o escopo de funcionalidade e o uso legal dos Produtos Licenciados, para os quais você deve suportar os custos resultantes, a menos que estabelecido de outra forma. A Pix4D notificará Você imediatamente por escrito se tomar conhecimento ou acreditar que qualquer instrução de processamento de dados Sua infringe a Lei de Proteção de Dados Europeia.

- 3.4. **Obrigações da Pix4D.** A Pix4D processará os Dados Pessoais do Cliente sob o EULA conforme as Leis de Proteção de Dados vigentes e suas instruções legais documentadas conforme descrito na Seção 3.2.
- 3.5. **Detalhes do Processamento.** O assunto do processamento de Dados Pessoais do Cliente pela Pix4D é a realização do EULA. Os tipos de dados pessoais e categorias de sujeitos dos dados, a frequência da transferência, a natureza do processamento, o propósito da transferência, o período de retenção dos dados e os detalhes do subprocessamento são especificados de modo mais aprofundado no Anexo C (Descrição da Transferência) deste DPA.

4. SOLICITAÇÕES DO SUJEITO DOS DADOS

Durante o Prazo, se a Pix4D receber uma solicitação do sujeito dos dados para exercer seus direitos de sujeito dos dados sob a Lei de Proteção de Dados Europeia, em relação aos Dados Pessoais do Cliente, a Pix4D vai: (i) orientar o sujeito dos dados a enviar sua solicitação a Você; (ii) imediatamente notificar Você; e (iii) não responder de outra forma àquela solicitação do sujeito dos dados diretamente, exceto conforme adequado (por exemplo, para orientá-lo a entrar em contato com Você) ou legalmente exigido, sem Sua autorização prévia. Além disso, a Pix4D vai, levando em conta a natureza do processamento, fornecer a Você assistência adicional razoável na medida possível para permitir que Você cumpra suas obrigações de proteção de dados com relação aos direitos do sujeito dos dados sob a Lei de Proteção de Dados Europeia. Sujeito a acordo anterior em texto entre as Partes, Você concorda em reembolsar a Pix4D por custos e despesas razoáveis incorridos pela Pix4D ao ajudar Você conforme esta Seção 4.

5. PESSOAL DA PIX4D

A Pix4D garantirá que qualquer pessoa autorizada pela Pix4D a processar Dados Pessoais do Cliente (incluindo sua equipe, agentes e subcontratados) esteja sob uma obrigação apropriada de confidencialidade (seja dever contratual ou estatutário) e tenha, em particular, concordado em não divulgar nenhum dos Dados Pessoais do Cliente a um terceiro nem processar tais dados para nenhum outro fim além de realizar as tarefas atribuídas a ela pela Pix4D de acordo com o EULA, ficando, ainda, entendido e acordado entre as Partes que a Pix4D continuará sendo responsável pela conduta de qualquer pessoal da Pix4D como é pela sua própria.

6. SUBPROCESSADORES

- 6.1. **Subprocessadores Autorizados.** Você concorda que a Pix4D pode contratar subprocessadores para processar Dados Pessoais do Cliente em Seu nome. Os subprocessadores atualmente contratados pela Pix4D e autorizados por Você são (i) Afiliadas da Pix4D e (ii) os terceiros mencionados na lista de subprocessadores da Pix4D disponível em <https://www.pix4d.com/legal>. Além disso, Você aqui concede autorização por escrito geral à Pix4D para indicar qualquer outro subprocessador de acordo com esta Seção 6 para realizar atividades de processamento específicas em nome da Pix4D.
- 6.2. **Oportunidade de Objetar à Mudança de Subprocessador.** Na medida em que a Lei de Proteção de Dados Europeia se aplica, a Pix4D informará Você de qualquer desafio almejado com relação à adição ou substituição de seus subprocessadores e Você terá a oportunidade de objetar a tais alterações com bases objetiva e razoavelmente justificáveis dentro de trinta (30) dias após ter sido notificado. Se Você apresentar uma objeção de modo oportuno, terá a oportunidade de discutir Suas preocupações com a Pix4D com o objetivo de alcançar uma resolução comercialmente razoável. Se não for possível chegar a

tal resolução, a Pix4D, a seu exclusivo critério, não indicará o novo subprocessador ou permitirá que você termine o EULA de acordo com as determinações de término do EULA sem responsabilidade à Pix4D (mas sem prejuízo a nenhuma tarifa incorrida por Você antes do término do EULA).

- 6.3. **Requisito para Contratação de Subprocessador.** Ao contratar qualquer subprocessador, a Pix4D garantirá que ele esteja vinculado a obrigações relacionadas à confidencialidade e à proteção de dados pelo menos tão rígidas quanto às determinações do EULA (incluindo este DPA) na medida aplicável à natureza das atividades de processamento fornecidas por esse subprocessador, ficando entendido e acordado que a Pix4D continuará sendo responsável pela conduta de todos os seus subprocessadores como é pela própria conduta.

7. SEGURANÇA DOS DADOS

A Pix4D vai implementar e manter medidas técnicas e organizacionais adequadas desenvolvidas para proteger Dados Pessoais do Cliente contra destruição acidental ou ilegal, perda, alteração, acesso ou divulgação não autorizada, incluindo, em particular e pelo menos as medidas estabelecidas no Anexo D (Medidas de Segurança) deste DPA (as "**Medidas de Segurança**"). As Medidas de Segurança incluem criptografar os Dados Pessoais do Cliente para ajudar a garantir a confidencialidade, a integridade, a disponibilidade e a resiliência contínuas dos sistemas e serviços da Pix4D, para ajudar a restaurar o acesso oportuno aos Dados Pessoais do Cliente após uma Violação de Dados e para teste regular de eficácia. Você é responsável por revisar as informações disponibilizadas pela Pix4D com relação à segurança de dados e fazer uma determinação independente quanto a se as Medidas de Segurança cumprem Seus requisitos e obrigações legais sob as Leis de Proteção de Dados. Você reconhece que as Medidas de Segurança estão sujeitas ao processo e desenvolvimento técnicos e que a Pix4D pode atualizar ou modificar as Medidas de segurança de tempos em tempos, desde que tais atualizações e modificações não resultem na degradação da segurança geral das Ofertas Licenciadas fornecidas a Você.

8. TRANSFERÊNCIAS DE DADOS PARA PAÍSES NÃO NA LISTA DE PERMITIDOS

- 8.1. **SCC DA UE.** As Partes concordam que a Pix4D pode transferir Dados Pessoais do Cliente a Países não na Lista de Permitidos com o objetivo de cumprir, ou em conexão com, o EULA. Quando a Pix4D transfere Dados Pessoais do Cliente sujeitos à Lei de Proteção de Dados Europeia (de volta) a Você, como controlador, localizado em um País não na Lista de Permitidos, as Partes concordam em estarem obrigadas pelo e cumprirem o Módulo Quatro (Transferir Processador para Controlador) do SCC da UE estabelecido no Anexo A (Módulo Quatro (Transferir Processador para Controlador) do SCC da UE) e compilado como segue (as "**Cláusulas P-C**"), incluindo qualquer emenda específica do país aplicável apresentada no Anexo B (Emendas Específicas do País ao SCC da UE) a este DPA, sendo a Pix4D o "exportador dos dados" e Você, o "importador dos dados":

(d) Cláusulas 1-6;

(e) A Cláusula 7 não se aplicará;

(f) Cláusula 8 com as determinações para o "Módulo Quatro", incluindo o parágrafo de introdução;

(g) Cláusula 10 com as determinações para o "Módulo Quatro";

- (h) Cláusula 11(a), mas sem as determinações da "Opção" da Cláusula 11(a);
- (i) Cláusula 12 com as determinações para o "Módulo Quatro"; na medida em que não está em conflito com o SCC da UE, a responsabilidade entre o importador dos dados e o exportador dos dados (mas não para os sujeitos dos dados) será limitada/excluída conforme a Seção 14 deste DPA;
- (j) As Cláusulas 14-15 com as determinações para o "Módulo Quatro", na medida em que o exportador dos dados combina dados pessoais recebidos do importador dos dados com os dados pessoais coletados pelo exportador dos dados no País na Lista de Permitidos;
- (k) Cláusula 16 com as determinações para o "Módulo Quatro";
- (l) Cláusula 17 com as determinações para o "Módulo Quatro", sendo a lei da França a lei acordada pelas Partes para os fins da Cláusula 17;
- (m) Cláusula 18 com as determinações para o "Módulo Quatro", sendo os tribunais da França a lei acordada pelas Partes para os fins da Cláusula 18.

8.2. **Anexos ao SCC da UE.** Os Anexos mencionados nas Cláusulas P-C serão formados como segue:

- (a) O Anexo I.A consistirá em:
 - i. as informações especificadas no EULA e fornecidas por Você no Formulário da Organização relevante, sendo a Pix4D o "exportador dos dados" atuando como "processador" e Você sendo o "importador dos dados" atuando como o "controlador".
 - ii. as informações de contato do exportador dos dados: Os dados de contato do exportador dos dados são Pix4D SA, Route de Renens 24, 1008 Prilly, Suíça. A equipe de proteção de dados do exportador dos dados pode ser contatada no seguinte endereço de e-mail: data_protection@pix4d.com. O executivo de proteção de dados do exportador dos dados pode ser contatado da seguinte forma: Parrot Drones, c/o Mr Victor Vuillard, 174 Quai de Jemmapes, 75010 Paris, França;
 - iii. as informações de contato do importador dos dados: Os dados de contato do importador dos dados, incluindo os dados de contato de seu executivo de proteção de dados, estão disponíveis ao exportador dos dados no Formulário da Organização relevante (em que esses detalhes foram fornecidos pelo importador dos dados) e/ou podem ser solicitados pelo exportador dos dados separadamente posteriormente em casos individuais;
 - iv. as atividades descritas no Anexo C (Descrição da Transferência) deste DPA;
 - v. as Partes concordam que a execução do EULA pelo importador dos dados e o exportador dos dados constituirá a execução destas Cláusulas P-C por ambas as Partes na Data Efetiva dos Termos.
- (b) O Anexo I.B consistirá na seção relevante do Anexo C (Descrição da Transferência);
- (c) O Anexo II consistirá no Anexo B (Medidas Técnicas e Organizacionais) deste DPA.
- (d) O Anexo III, quando aplicável, consistirá na lista da Pix4D de subprocessadores disponível em <https://www.pix4d.com/legal>.

8.3. **Avaliação de Impacto da Transferência.** O Cliente reconhece que, no seu melhor conhecimento, as transferências planejadas de dados pessoais da Pix4D

(de volta) ao Cliente são permitidas sob a lei vigente e as Partes não têm motivo para crer que as transferências pretendidas não são autorizadas.

- 8.4. **Indenização.** Cada Parte indenizará a outra Parte em caso de reivindicações de terceiros devido a uma violação de suas obrigações sob as Cláusulas P-C.

9. VIOLAÇÕES DE DADOS

Ao tomar conhecimento de uma Violação de Dados, a Pix4D deverá: (i) notificar Você sem atraso indevido e, quando viável, em qualquer caso não após quarenta e oito (48) horas do momento em que tomou conhecimento da Violação de Dados; (ii) fornecer informações oportunas relacionadas à Violação de Dados conforme elas se tornarem conhecidas ou conforme for razoavelmente solicitado por Você; e (iii) imediatamente tomar medidas razoáveis para conter e investigar qualquer Violação de Dados. A notificação da Pix4D de, ou a resposta a, uma Violação de Dados sob esta Seção 9 não será interpretada como um reconhecimento da Pix4D de qualquer falha ou responsabilidade com relação à Violação de Dados.

10. SOLICITAÇÕES DE ACESSO A DADOS POR PARTE DO GOVERNO

Ao processar Dados Pessoais do Cliente como Seu processador sob a Lei de Proteção de Dados Europeia, a Pix4D não fornece a agências do governo nem às autoridades, incluindo a polícia, acesso ou informações sobre Contas da Pix4D, incluindo Dados do Cliente, a menos que isso seja exigido pela lei vigente. Os custos associados a responder a uma solicitação compulsória (seja por meio de intimação, ordem judicial, mandado de busca ou outro processo legal válido) de qualquer agência do governo ou autoridade, incluindo polícia, para acessar informações sobre uma Conta da Pix4D, incluindo Dados do Cliente, que pertencem a Você e/ou aos Usuários Autorizados serão pagos por Você.

11. REVISÃO E AUDITORIA DE CONFORMIDADE

A Pix4D fornecerá a Você todas as informações razoavelmente necessárias para demonstrar conformidade com suas obrigações sob este DPA e permitir e contribuir para auditorias, incluindo inspeções, realizadas por Você ou um auditor independente indicado por Você para verificar a conformidade da Pix4D com suas obrigações sob este DPA, sujeito a acordos de confidencialidade costumeiros. Além disso, a Pix4D poderá fornecer a Você, gratuitamente, sem solicitação ou mediante pedido, qualquer relatório de auditoria preparado pelo auditor da Pix4D confirmando a conformidade da Pix4D com este DPA.

12. AVALIAÇÕES DE IMPACTO E CONSULTORIAS

Na medida exigida sob as Leis de Proteção de Dados vigentes, a Pix4D deverá, levando em conta a natureza do processamento e das informações disponíveis à Pix4D, fornecer todas as informações razoavelmente solicitadas sobre as Ofertas Licenciadas para permitir que Você realize avaliações de impacto de proteção de dados ou consultas prévias com autoridades de proteção de dados conforme exigido pelas Leis de Proteção de Dados. Sujeito a acordo anterior em texto entre as Partes, Você reembolsará a Pix4D por custos e despesas razoáveis incorridos pela Pix4D ao ajudar Você conforme esta Seção 12.

13. DEVOLUÇÃO OU EXCLUSÃO DE DADOS

Ao término ou expiração do EULA, a Pix4D deverá (conforme Sua escolha) excluir (incluindo por meio de anonimização) ou devolver a Você todos os Dados Pessoais do Cliente (incluindo cópias) em sua posse ou controle, exceto que esse requisito não deve se aplicar na medida em que a Pix4D é exigida por lei a reter alguns ou todos os Dados Pessoais do Cliente, ou Dados Pessoais do Cliente que

ela tem arquivados em sistemas de backup, Dados Pessoais do Cliente que a Pix4D deve isolar com segurança, proteger contra mais processamento e por fim excluir conforme as políticas de exclusão da Pix4D, exceto na medida exigida pela lei vigente.

14. LIMITAÇÃO DE RESPONSABILIDADE

Exceto conforme estabelecido nas Cláusulas P-C apresentadas nas Seções 8.1 e 8.2 e exceto conforme explicitamente acordado neste DPA, a responsabilidade da Pix4D, com relação à Sua responsabilidade, é excluída na medida permitida sob a lei vigente.

15. DIVERSOS

- 15.1. **Emendas.** Qualquer emenda a este DPA será feita por escrito e devidamente assinada por um representante autorizado das Partes.
- 15.2. **Conflitos.** No caso de qualquer conflito ou inconsistência entre este DPA e o EULA quanto ao processamento de Dados Pessoais do Cliente, as determinações dos documentos a seguir (em ordem de precedência) prevalecerão: (i) SCC da UE; (ii) este DPA; e, por fim, (iii) o EULA
- 15.3. **Separabilidade.** Se alguma determinação do DPA for considerada inexecutável por qualquer motivo, ela deverá ser ajustada, em vez de anulada, se possível, para alcançar a intenção legal e econômica das Partes na máxima extensão possível. Em qualquer caso, todas as demais determinações do DPA continuarão sendo válidas e executáveis na máxima extensão possível.
- 15.4. **Avisos.** Para os fins de todas as comunicações por escrito entre as Partes, qualquer aviso ou outra comunicação feito em relação ao EULA será por escrito (sendo a forma eletrônica considerada satisfatória) e deverá ser enviado por e-mail aos endereços abaixo:

Se para a Pix4D: e-mail: legal@pix4d.com.

Se para Você: o endereço de e-mail registrado na Sua Conta. Em caso de alteração, é Sua exclusiva responsabilidade informar a Pix4D de Seus novos dados de contato. Para isso, Você pode entrar em contato com a equipe de suporte da Pix4D por meio do site <https://support.pix4d.com> ou atualizar Seus dados de contato na Sua Conta.

Quando e se usado, o sistema de comunicação eletrônica empregado pela Pix4D servirá como a prova única para o conteúdo e o momento da entrega e do recebimento de tais comunicações eletrônicas.

- 15.5. **Custos.** Cada Parte deverá pagar os próprios custos associados à sua conformidade com este DPA, incluindo as Cláusulas P-C, conforme aplicável.

16. LEI VIGENTE – RESOLUÇÃO DE DISPUTA

- 16.1. **Lei Vigente.** Independentemente da lei vigente do EULA, este DPA será exclusivamente regido e interpretado conforme a lei substantiva da Suíça, em que (i) convenções internacionais, incluindo a Convenção das Nações Unidas sobre Contratos para a Venda Internacional de Mercadorias de 11 de abril de 1980 (CISG) e (ii) regras suíças de conflito legal são explicitamente excluídas da

aplicação a este DPA.

16.2. **Jurisdição e Local.** Independentemente do local de jurisdição do EULA, os tribunais ordinários de Lausanne, Suíça, terão jurisdição exclusiva com relação a qualquer disputa decorrente entre as Partes devido ou com relação a este DPA.

17. DETERMINAÇÕES ADICIONAIS PARA INFORMAÇÕES PESSOAIS NA CALIFÓRNIA

17.1. **Escopo e Aplicabilidade.** Esta Seção 17 do DPA se aplica além dos termos deste DPA, na medida em que a Pix4D processa Informações Pessoais da Califórnia sob o EULA sujeito à CCPA. No caso de qualquer conflito ou ambiguidade entre esta Seção 17 e qualquer outro termo deste DPA, esta Seção Section 17 terá precedência, mas apenas na medida da aplicabilidade desta Seção à Pix4D.

17.2. **Funções das Partes.** Ao processar Informações Pessoais da Califórnia de acordo com as Suas instruções, as Partes reconhecem e concordam que Você é um Negócio e a Pix4D é um Prestador de Serviço para os fins da CCPA.

17.3. **Responsabilidades.** As Partes concordam que a Pix4D processará Informações Pessoais da Califórnia como um Prestador de Serviço estritamente para a finalidade de licenciar as Ofertas Licenciadas sob o EULA (o "**Objetivo de Negócio**") ou conforme permitido de outra forma pela CCPA.

18. DEFINIÇÕES

Termos Adicionais	conforme o sentido na página inicial.
Usuários Autorizados	significa as pessoas que Você permite que usem os Produtos Licenciados de acordo com o EULA. Para clareza, Usuários Autorizados podem incluir Seus funcionários, Suas afiliadas e outros terceiros fora de Sua entidade que tenham sido devidamente autorizados pelo Seu administrador da conta para tornarem-se membros de uma Organização, em que Você atual como controlador de tais outros terceiros.
Negócio	terá o sentido atribuído no CCPA.
Propósito de Negócios	conforme o significado na Seção 17.3.
Informações Pessoais da Califórnia	significa Dados Pessoais sujeitos à proteção da CCPA.
CCPA	significa o Código Civil da Califórnia Seç. 1798.100 et seq., também conhecida como Lei de Privacidade do Consumidor da Califórnia de 2018.
CNIL	significa a Commission Nationale de l'Informatique et des Libertés conforme o significado na Seção 8.2
Consumidor	terá o sentido atribuído no CCPA.
Controlador	significa a pessoa física ou jurídica, autoridade pública, agência ou outro órgão que, sozinho ou junto com outros,

	determina os propósitos e os meios de processamento de dados pessoais.
Dados do Cliente	significa dados fornecidos por ou em nome Seu ou de Usuários Finais por meio das Ofertas Licenciadas sob a Conta.
Dados Pessoais do Cliente	significa os dados pessoais contidos nos Dados do Cliente, incluindo qualquer categoria especial de dados pessoais.
Violação de Dados	significa uma violação de segurança que leva a destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a dados pessoais transmitidos, armazenados ou de outra forma processados pela Pix4D, incluindo, entre outros, qualquer violação do <u>Anexo D (Medidas de Segurança)</u> .
Leis de Proteção de Dados	significa todas as leis e regulamentos de proteção de dados aplicáveis à Pix4D ou Seu processamento de Dados Pessoais do Cliente sob o EULA, incluindo, conforme aplicável, a Lei de Proteção de Dados Europeia e a Lei de Proteção de Dados Não Europeia.
Sujeito dos Dados	significa qualquer pessoa física identificada ou identificável à qual os dados pessoais se relacionam.
Solicitação do Sujeito dos Dados	conforme o significado na Seção 4.
DPA	conforme o sentido na página inicial.
EEA	significa o Espaço Econômico Europeu
EULA	conforme o sentido na página inicial.
SCC da UE	significa o padrão contratual, conforme aprovado pela Decisão da Comissão Europeia de 4 de junho de 2021 [C(2021)3972 final] sobre cláusulas contratuais padrão para a transferência de dados pessoais a outros países conforme o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho e quaisquer emendas aos mesmos.
Lei de Proteção de Dados Europeia	significa, conforme aplicável, (a) os RGPD e qualquer legislação local, regional ou nacional implementando os RGPD; (b) os RGPD do Reino Unido; e (c) o DPA da Suíça e, em cada caso, qualquer versão nova ou revisada que possa entrar em vigor durante o Prazo.
FDPIC	significa o Comissário Federal de Proteção de Dados e Informação da Suíça conforme o significado na Seção 8.2
RGPD	significa o Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 sobre a proteção de pessoas físicas com relação ao processamento de dados pessoais e à livre movimentação de tais dados e revogando a Diretiva 95/46/CE, qualquer

		versão nova ou revisada dos mesmos que possam entrar em vigor durante o Prazo.
Termos Gerais		conforme o sentido na página inicial.
Lei de Proteção de Dados Não Europeia		significa leis de proteção de dados ou privacidade em vigor fora do EEE, do Reino Unido e da Suíça, incluindo, entre outras, a CCPA.
Formulário de Organização	da	significa as configurações da Organização dentro do Gerenciamento de Usuário Empresarial fornecidas pela Pix4D para o registro da Sua Conta.
Partes		conforme o sentido na página inicial.
Cláusulas P-C		significa o Módulo Quatro (Transferência do Processador para o Controlador) do SCC da UE conforme compilado e estabelecido nas Seções 8.1 e 8.2 deste DPA.
Pix4D, Nós, Nosso		Pix4D SA, uma empresa Suíça de sociedade por ações (<i>société anonyme</i>), registrada na Suíça sob o número CHE-207.009.701, tendo sua sede registrada em Route de Renens 24, 1008 Prilly, Suíça.
Medidas de Segurança		significa as medidas técnicas e organizacionais de segurança conforme descritas no <u>Anexo D</u> (<i>Medidas de Segurança</i>).
Prestador de Serviço		terá o sentido atribuído no CCPA.
DPA da Suíça		significa a Lei Federal da Suíça sobre Proteção de Dados de 19 de junho de 1992 e o Regulamento Suíço sobre a Lei Federal de Proteção de Dados de 14 de junho de 1993 e, em cada caso, qualquer versão nova ou revisada dos mesmos que possa entrar em vigor durante o prazo.
Prazo		significa o período da Data Efetiva dos Termos até o fim do fornecimento por parte da Pix4D das Ofertas Licenciadas, incluindo, se aplicável, qualquer período durante o qual o fornecimento das Ofertas Licenciadas pode ser suspenso e qualquer período após o término durante o qual a Pix4D possa continuar fornecendo as Ofertas Licenciadas para fins de transição.
Data Efetiva dos Termos		significa a data em que Você aceitou, as Partes de outra forma concordaram com, este DPA.
RGPD do Reino Unido		significa o RGPD da UE conforme emendas e incorporação à lei do Reino Unido sob a Lei (de Retirada) da União Europeia do Reino Unido 2018, e legislação secundária aplicável feita sob essa lei e qualquer versão nova ou revisada que possa entrar em vigor durante o Prazo.
Países na lista de Permitidos	de	significa: - <i>para Dados Pessoais do Cliente sujeitos aos RGPD: o EEE ou um país ou território sujeito a uma decisão de</i>

adequação da Comissão Europeia sob o Artigo 45(1) Dos RGPD;

- *para Dados Pessoais do Cliente sujeitos aos RGPD do Reino Unido:* o Reino Unido ou um país ou território sujeito aos regulamentos de adequação sob o Artigo 45(1) dos RGPD do Reino Unido e Seção 17A da Lei de Proteção de Dados 2018; e/ou
- *para Dados Pessoais do Cliente sujeitos ao DPA da Suíça:* A Suíça ou um país ou território que (i) esteja incluído na lista de Estados cuja legislação garante um nível adequado de proteção conforme publicado pelo Comissário Federal da Proteção de Dados e Informação da Suíça ou, conforme o caso, (ii) seja o sujeito de uma decisão de adequação pelo Conselho Federal Suíço sob o DPA da Suíça.

Você e Seu

significa a pessoa jurídica que está licenciando as Ofertas Licenciadas sob o EULA para uso por seus Usuários Autorizados.

Os termos "dados pessoais", "sujeito dos dados", "processamento", "controlador" e "processador" como usados neste DPA têm os significados atribuídos nos RGPD independentemente de A Lei de Proteção de Dados Europeia ou a Lei de Proteção de Dados Não Europeia se aplicar.

Anexos:

Anexo A: Módulo Quatro (Transferência do Processador para o Controlador) do SCC da UE

Anexo B: Emendas Específicas do País ao SCC da UE

Anexo C: Descrição da Transferência

Anexo D: Medidas de Segurança

Cláusula 8

Resguardos de proteção de dados

O exportador dos dados garante que envidou os esforços razoáveis para determinar que o importador dos dados é capaz, implementando as medidas técnicas e organizacionais apropriadas, de cumprir suas obrigações sob estas Cláusulas.

8.1 Instruções

- (a) O exportador dos dados deve processar os dados pessoais apenas conforme instruções documentadas do importador dos dados atuando como seu controlador.
- (b) O exportador dos dados deve imediatamente informar o importador dos dados se não conseguir seguir essas instruções, incluindo se as instruções infringirem o Regulamento (UE) 2016/679 ou outra lei de proteção de dados da União ou Estado Membro.
- (c) O importador dos dados deve evitar qualquer ação que possa impedir o exportador dos dados de cumprir suas obrigações sob o Regulamento (EU) 2016/679, incluindo no contexto de subprocessamento ou com relação à cooperação com as autoridades supervisoras competentes.
- (d) Depois do fim da prestação dos serviços de processamento, o exportador dos dados deverá, conforme o importador dos dados escolher, excluir todos os dados pessoais em nome do importador dos dados e certificar ao importador dos dados de que fez isso, ou devolver ao importador dos dados todos os dados pessoais processados em nome dele e excluir as cópias existentes.

8.2 Segurança do processamento

- (a) As Partes devem implementar medidas técnicas e organizacionais apropriadas para garantir a segurança dos dados, incluindo durante a transmissão, e proteção contra uma violação de segurança que leve a destruição acidental ou ilícita, perda, alteração, acesso ou divulgação não autorizado (doravante, "violação de dados pessoais"). Ao avaliar o nível adequado de segurança, é preciso levar em conta a tecnologia, os custos de implementação, a natureza dos dados pessoais ⁽²⁾, a natureza, o escopo, o contexto e os fins do processamento e os riscos envolvidos no processamento dos sujeitos dos dados, e, em particular, considerar ter recurso para criptografia ou pseudonimização, incluindo durante a transmissão, em que o objetivo do processamento pode ser atendido dessa maneira.
- (b) O exportador dos dados deve ajudar o importador dos dados a garantir a segurança adequada dos dados conforme o parágrafo (a). No caso de violação

¹ Quando o exportador de dados for um processador sujeito ao Regulamento (UE) 2016/679 agindo em nome de um órgão ou uma instituição da União como controlador, confiança nestas Cláusulas ao contratar outro processador (subprocessamento) não sujeito ao Regulamento (UE) 2016/679 também garante conformidade com o Artigo 29(4) do Regulamento (EU) 2018/1725 do Parlamento Europeu e do Conselho de 23 de outubro de 2018 sobre a proteção de pessoas físicas com relação ao processamento de dados pessoais por instituições, órgãos, escritórios e agências da União e a livre movimentação desses dados, e revogando o Regulamento (CE) N° 45/2001 e a Decisão N° 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), na medida em que essas Cláusulas e as obrigações de proteção de dados conforme estabelecidas no contrato ou outro ato legal entre o controlador e o processador de acordo com o Artigo 29(3) do Regulamento (UE) 2018/1725 estão alinhadas. Esse será, em particular, o caso quando o controlador e o processador se basearem nas cláusulas contratuais padrão incluídas na Decisão 2021/915.

² Isso inclui se a transferência e o processamento adicional envolvem dados pessoais que revelam origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas ou associação a sindicato, dados genéticos ou biométricos para os fins de identificar uma pessoa de modo exclusivo, dados referentes à saúde ou à vida sexual ou orientação sexual de uma pessoa ou dados relativos a condenações criminais ou delitos.

de dados pessoais com relação aos dados pessoais processados pelo exportador dos dados sob estas Cláusulas, o exportador dos dados deverá notificar o importador dos dados sem atraso indevido depois de tomar conhecimento do fato e ajudar o importador dos dados a lidar com a violação.

- (c) O exportador dos dados deve garantir que as pessoas autorizadas a processar os dados pessoais tenham se comprometido elas mesmas com a confidencialidade ou estejam sob uma obrigação estatutária apropriada de confidencialidade.

8.3 Documentação e conformidade

- (a) As Partes devem poder demonstrar conformidade com estas Cláusulas.
- (b) O exportador dos dados deve disponibilizar ao importador dos dados todas as informações necessárias para demonstrar conformidade com suas obrigações sob estas Cláusulas e permitir e contribuir para auditorias.

Cláusula 9

Uso de subprocessadores

N/A

Cláusula 10

Direitos do sujeito dos dados

As Partes devem ajudar umas às outras a responder às perguntas e solicitações feitas pelos sujeitos dos dados sob a lei local aplicável ao importador dos dados ou, para processamento de dados pelo exportador dos dados na UE, sob o Regulamento (UE) 2016/679.

Cláusula 11

Reparação

- (a) O importador dos dados deve informar os sujeitos dos dados em um formato transparente e facilmente acessível, por meio de aviso individual ou no site, sobre um ponto de contato autorizado a lidar com as reclamações. Ele deve lidar imediatamente com qualquer reclamação que receber de um sujeito dos dados.

[OPÇÃO: O importador dos dados concorda que os sujeitos dos dados também podem fazer uma reclamação com um órgão de resolução de disputa independente ⁽³⁾ sem custo ao sujeito dos dados. Ele deverá informar os sujeitos dos dados do modo estabelecido no parágrafo (a) de tal mecanismo de reparação e que ele não precisa usá-lo ou seguir uma sequência específica ao buscar reparação.]

Cláusula 12

Responsabilidade

- (a) Cada parte será responsável perante as outras por quaisquer danos que cause às outras Partes por qualquer violação destas Cláusulas.
- (b) Cada Parte será responsável perante o sujeito dos dados, e o sujeito dos dados terá direito a receber compensação por qualquer dano material ou não material

³ O importador dos dados poderá oferecer resolução de disputa independente por meio de um órgão de arbitragem apenas se estiver estabelecido em um país que tenha ratificado a Convenção de Nova York sobre Imposição de Prêmios de Arbitragem.

que a Parte cause ao sujeito dos dados ao violar os direitos do terceiro beneficiário sob estas Cláusulas. Isso não prejudica a responsabilidade do exportador dos dados sob o Regulamento (UE) 2016/679.

- (c) Quando mais de uma parte for responsável por qualquer dano causado ao sujeito dos dados como resultado de uma violação destas Cláusulas, todas as Partes responsáveis serão responsáveis de modo conjunto e separado e o sujeito dos dados terá direito a abrir um processo no tribunal contra qualquer uma dessas Partes.
- (d) As Partes concordam que se uma Parte for considerada responsável sob o parágrafo (c), ela terá direito a reivindicar de volta das outras Partes aquela parcela da compensação que corresponde à responsabilidade da outra Parte pelo dano.
- (e) O importador dos dados não pode invocar a conduta de um processador ou subprocessador para evitar sua própria responsabilidade.

Cláusula 13

Supervisão

N/A

SEÇÃO III – LEIS LOCAIS E OBRIGAÇÕES EM CASO DE ACESSO POR AUTORIDADES PÚBLICAS

Cláusula 14

Leis e práticas locais que afetam a conformidade com as Cláusulas

(quando o processador da UE combina os dados pessoais recebidos do controlador do outro país com os dados pessoais coletados pelo processador na UE)

- (a) As Partes garantem que não têm motivo para crer que as leis e as práticas no outro país de destino aplicável ao processamento de dados pessoais pelo importador dos dados, incluindo quaisquer requisitos de divulgar dados pessoais ou medidas autorizando o acesso por autoridades públicas, impedem o importador dos dados de cumprir suas obrigações sob estas Cláusulas. Isso é baseado no entendimento de que leis e práticas que respeitam a essência dos direitos e liberdades fundamentais e não excedem o que é necessário e proporcional em uma sociedade democrática para proteger um dos objetivos listados no Artigo 23(1) do Regulamento (UE) 2016/679 não estão em contradição com estas Cláusulas.
- (b) As Partes declaram que, ao fornecer a garantia no parágrafo (a), elas devidamente levaram em conta, em particular, os seguintes elementos:
 - (i) as circunstâncias específicas da transferência, incluindo a extensão da cadeia de processamento, o número de pessoas envolvidas nos canais de transmissão usados; transferências adiante pretendidas; o tipo de destinatário; o propósito do processamento; as categorias e o formato dos dados pessoais transferidos; o setor econômico em que a transferência ocorre; o local de armazenamento dos dados transferidos;
 - (ii) as leis e as práticas do outro país de destino, incluindo aquelas que exigem a divulgação dos dados a autoridades públicas ou autorizando acesso por

essas autoridades, relevantes à luz das circunstâncias específicas da transferência e as limitações e proteções aplicáveis ⁽⁴⁾;

- (iii) qualquer proteção contratual, técnica ou organizacional estabelecida para suplementar as proteções sob estas Cláusulas, incluindo medidas aplicadas durante a transmissão e o processamento de dados pessoais no país de destino.
- (c) O importador de dados garante que, ao realizar a avaliação sob o parágrafo (b), ele envidou seus melhores esforços para fornecer ao exportador dos dados informações relevantes e concorda que continuará a cooperar com o exportador dos dados para garantir conformidade com estas Cláusulas.
- (d) As Partes concordam em documentar a avaliação sob o parágrafo (b) e disponibilizá-la à autoridade supervisória competente mediante solicitação.
- (e) O importador dos dados concorda em notificar o exportador dos dados imediatamente se, após terem acordado com estas Cláusulas e durante o contrato, ele tiver motivo para crer que está ou passou a estar sujeito às leis ou práticas não alinhadas aos requisitos sob o parágrafo (a), incluindo após uma mudança nas leis do outro país ou uma medida (como solicitação de divulgação) indicando uma aplicação de tais leis na prática que não está alinhada com os requisitos no parágrafo (a).
- (f) Após uma notificação de acordo com o parágrafo (e), ou se o exportador dos dados de outra forma tiver motivo para acreditar que o importador dos dados não pode mais cumprir suas obrigações sob estas Cláusulas, o exportador dos dados deverá imediatamente identificar medidas adequadas (por exemplo, medidas técnicas ou organizacionais para garantir a segurança e a confidencialidade) a serem adotadas pelo exportador dos dados e/ou o importador dos dados para lidar com a situação. O exportador dos dados deverá suspender a transferência de dados se considerar que nenhuma proteção adequada para essa transferência pode ser garantida ou se instruído pela autoridade supervisória competente a fazer isso. Nesse caso, o exportador dos dados terá direito a terminar o contrato, na medida em que se refere ao processamento de dados pessoais sob estas Cláusulas. Se o contrato envolver mais de duas Partes, o exportador dos dados poderá exercer seu direito de término apenas com relação à Parte relevante, a menos que as Partes tenham acordado de outra forma. Quando o contrato for terminado conforme esta Cláusula, a Cláusula 16(d) e (e) serão aplicadas.

Cláusula 15

Obrigações do importador dos dados no caso de acesso por autoridades públicas

(quando o processador da UE combina os dados pessoais recebidos do controlador do outro país com os dados pessoais coletados pelo processador na UE)

15.1 Notificação

⁴ Com relação ao impacto dessas leis e práticas em conformidade com estas Cláusulas, diferentes elementos podem ser considerados parte de uma avaliação geral. Esses elementos podem incluir experiência prática relevante e documentada com casos anteriores de solicitações de divulgação de autoridades públicas, ou a ausência de tais solicitações, cobrindo um período suficientemente representativo. Isso se refere, em particular, a registros internos ou outra documentação, traçados de modo contínuo conforme a devida diligência e certificados no nível da gerência sênior, desde que essas informações possam ser legalmente compartilhadas com terceiros. Quando essa experiência prática é tomada como base para concluir que o importador dos dados não será impedido de cumprir estas Cláusulas, é preciso embasar essa decisão por outros elementos objetivos relevantes e as Partes devem considerar cuidadosamente se esses elementos juntos têm peso suficiente, em termos de confiabilidade e representatividade, para embasar a conclusão. Em particular, as Partes devem levar em conta se a experiência prática delas é corroborada e não contradita por informações confiáveis disponíveis ao público ou de outra forma acessíveis sobre a existência ou a ausência de solicitações dentro do mesmo setor e/ou a aplicação da lei na prática, como jurisprudência e relatórios de órgãos de supervisão independentes.

- (a) O importador dos dados concorda em notificar o exportador dos dados e, quando possível, o sujeito dos dados imediatamente (se necessário, com a ajuda do exportador dos dados) se:
 - (i) receber uma solicitação compulsória de uma autoridade pública, incluindo autoridades judiciais, sob as leis do país de destino para a divulgação de dados pessoais transferidos conforme estas Cláusulas; essa notificação deverá incluir informações sobre os dados pessoais solicitados, a autoridade solicitante, a base legal da solicitação e a resposta dada; ou
 - (ii) tomar conhecimento de qualquer acesso direto por autoridades públicas a dados pessoais transferidos conforme estas Cláusulas de acordo com as leis do país de destino; essa notificação incluirá todas as informações disponíveis ao importador.
- (b) Se o importador dos dados for proibido de notificar o exportador dos dados e/ou o sujeito dos dados sob as leis do país de destino, o importador dos dados concorda em envidar seus melhores esforços para obter uma isenção da proibição com o objetivo de comunicar o máximo de informações possível assim que possível. O importador dos dados concorda em documentar seus melhores esforços para poder demonstrá-los mediante solicitação do exportador dos dados.
- (c) Quando permitido sob as leis do país de destino, o importador dos dados concorda em fornecer ao exportador dos dados, a intervalos regulares durante o contrato, o máximo de informações relevantes possível sobre as solicitações recebidas (em particular, número de solicitações, tipo de dados solicitados, autoridades solicitantes, se as solicitações foram contestadas e o resultado de tais contestações etc.).
- (d) O importador dos dados concorda em preservar as informações conforme os parágrafos (a) a (c) durante o contrato e disponibilizá-las à autoridade supervisória competente mediante solicitação.
- (e) Os Parágrafos (a) a (c) não afetam a obrigação do importador dos dados com relação à Cláusula 14(e) e à Cláusula 16 de informar o exportador dos dados imediatamente quando não puder cumprir essas Cláusulas.

15.2 Análise de legalidade e minimização de dados

- (a) O importador dos dados concorda em revisar a legalidade da solicitação de divulgação, em particular se ela permanece dentro dos poderes concedidos à autoridade pública solicitante, e contestar a solicitação se, após avaliação cuidadosa, concluir que há bases razoáveis para considerar que a solicitação é ilegal sob as leis do país de destino, obrigações vigentes sob a lei internacional e princípios de respeito internacional. O importador dos dados deve, sob as mesmas condições, buscar possibilidades de recurso. Ao contestar uma solicitação, o importador dos dados deve buscar medidas provisórias com o objetivo de suspender os efeitos da solicitação até a autoridade judicial competente ter decidido sobre seus méritos. Ele não deve divulgar os dados pessoais solicitados até que seja exigido que faça isso sob as regras processuais aplicáveis. Esses requisitos não afetam as obrigações do importador dos dados sob a Cláusula 14(e).

- (b) O importador dos dados concorda em documentar sua avaliação legal e qualquer contestação da solicitação de divulgação e, na medida permitida pelas leis do país de destino, disponibilizar a documentação ao exportador dos dados. Ele também deverá disponibilizá-la à autoridade supervisória competente mediante solicitação.
- (c) O importador dos dados concorda em fornecer a quantidade mínima de informações permitida ao responder a uma solicitação de divulgação com base em uma interpretação razoável da solicitação.

SEÇÃO IV – DETERMINAÇÕES FINAIS

Cláusula 16

Não conformidade com as Cláusulas e término

- (a) O importador dos dados deve informar imediatamente o exportador dos dados se não puder cumprir estas Cláusulas por qualquer motivo.
- (b) No caso de o importador dos dados violar uma destas Cláusulas ou não puder cumprir estas Cláusulas, o exportador dos dados deverá suspender a transferência de dados pessoais ao importador dos dados até que a conformidade seja novamente garantida ou terminar o contrato. Isso não afeta a Cláusula 14(f).
- (c) O exportador dos dados terá direito a terminar o contrato, na medida em que se refere ao processamento de dados pessoais sob estas Cláusulas, em que:
 - (i) o exportador dos dados suspendeu a transferência de dados pessoais ao importador dos dados conforme o parágrafo (b) e a conformidade com estas Cláusulas não é restaurada dentro de um período razoável e, em qualquer caso, dentro de um mês da suspensão;
 - (ii) o importador dos dados está em violação considerável ou persistente destas Cláusulas; ou
 - (iii) o importador dos dados falha em cumprir uma decisão compulsória de um tribunal ou autoridade supervisória competente sobre suas obrigações sob estas Cláusulas.

Nesses casos, ele deverá informar a autoridade supervisória competente de tal não conformidade. Quando o contrato envolver mais de duas Partes, o exportador dos dados poderá exercer seu direito de término apenas com relação à Parte relevante, a menos que as Partes tenham acordado de outra forma.

- (d) Dados pessoais coletados pelo exportador dos dados na UE que foram transferidos antes do término do contrato conforme o parágrafo (c) deverão ser imediatamente excluídos em sua totalidade, incluindo qualquer cópia dos mesmos. O importador dos dados deve certificar a exclusão dos dados ao exportador dos dados. Até os dados serem excluídos ou devolvidos, o importador dos dados deve continuar garantindo a conformidade com estas Cláusulas. No caso de leis locais aplicáveis ao importador dos dados que proíbam a devolução ou a exclusão dos dados pessoais transferidos, o importador dos dados garante que continuará a garantir conformidade com estas Cláusulas e somente processará os dados na medida e pelo tempo necessário sob a lei local.

- (e) Qualquer uma das Partes pode revogar sua concordância em estar obrigada pelas Cláusulas quando (i) a Comissão Europeia adotar uma decisão conforme o Artigo 45(3) do Regulamento (UE) 2016/679 que cubra a transferência de dados pessoais aos quais estas Cláusulas se aplicam; ou (ii) o Regulamento (UE) 2016/679 passar a fazer parte da estrutura legal do país ao qual os dados pessoais são transferidos. Isso não afeta outras obrigações que se aplicam ao processamento em questão sob o Regulamento (UE) 2016/679.

Cláusula 17

Lei vigente

Estas Cláusulas serão regidas pela lei de um país que permite direitos de terceiros beneficiários. As Partes concordam que essa será a lei de _____ (*especificar o país*).

Cláusula 18

Escolha de fórum e jurisdição

Qualquer disputa decorrente destas Cláusulas deverá ser resolvida pelos tribunais de _____ (*especificar o país*) **APÊNDICE**

NOTA EXPLICATIVA:

Deve ser possível distinguir claramente as informações aplicáveis a cada transferência ou categoria de transferência e, nesse sentido, determinar as respectivas funções das Partes como exportador dos dados e/ou importador dos dados. Isso não necessariamente exige preencher e assinar apêndices separados para cada transferência/categoria de transferência e/ou relação contratual quando essa transparência pode ser obtida com um apêndice. Porém, quando for necessário para garantir clareza suficiente, apêndices separados devem ser usados.

ANEXO I

A. LISTA DE PARTES

Exportadores de dados: *[Identidade e dados de contato dos exportador dos dados e, quando aplicável, o respectivo diretor e/ou representante de proteção de dados na União Europeia]*

1.

Nome: _____

Endereço: _____

Nome, cargo e dados de contato da pessoa de contato:

Atividades relevantes para os dados transferidos sob estas Cláusulas:

Assinatura e data: _____

Função (controlador/processador):

2.

Importadores dos dados: *[Identidade e dados de contato dos importador dos dados, incluindo qualquer pessoa de contato responsável pela proteção dos dados]*

1.

Nome: _____

Endereço: _____

Nome, cargo e dados de contato da pessoa de contato:

Atividades relevantes para os dados transferidos sob estas Cláusulas:

Assinatura e data: _____

Função (controlador/processador):

2.

B. DESCRIÇÃO DE TRANSFERÊNCIA

Categorias de sujeitos dos dados cujos dados pessoais são transferidos

Categorias de dados pessoais transferidos

Dados confidenciais transferidos (se aplicável) e restrições ou proteções aplicadas que levam totalmente em conta a natureza dos dados e os riscos envolvidos, como, por exemplo, limitação de finalidade estrita, restrições de acesso (incluindo acesso apenas para equipe que tenha feito treinamento especializado), manter um registro do acesso aos dados, restrições para transferências adiante ou medidas de segurança adicionais.

A frequência da transferência (por exemplo, se os dados são transferidos uma só vez ou de modo contínuo).

Natureza do processamento

Propósitos da transferência de dados e processamento adicional

O período para o qual os dados pessoais serão retidos ou, se isso não for possível, os critérios usados para determinar esse período

Para transferências a (sub)processadores, especificar também o assunto, a natureza e a duração do processamento

Anexo B: Emendas Específicas do País ao SCC da UE

Suíça

Para os fins do DPA da Suíça, em que transferências de Dados Pessoais do Cliente sob o EULA estão sujeitas aos RGPD e ao DPA da Suíça, as Cláusulas P-C, conforme aplicável de acordo com as Seções 8.1 e 8.2 deste DPA serão aplicadas com as seguintes emendas (para evitar dúvida, estas emendas não afetam as Cláusulas P-C conforme aplicáveis para os fins dos RGPD):

- Referências ao "Regulamento (UE) 2016/679" ou "àquele Regulamento" devem ser interpretadas como referências ao DPA da Suíça na medida aplicável.
- Referências ao "Regulamento (UE) 2018/1725" são removidas.
- Referências a "União", "UE" e "Estado Membro da UE" devem ser interpretadas como significando a Suíça.
- A Cláusula 17 é substituída para declarar que "Estas Cláusulas são regidas pelas leis da Suíça" na medida em que as transferências são regidas pelo DPA da Suíça.
- A Cláusula 18 é substituída para declarar:
"Qualquer disputa decorrente destas Cláusulas com relação à DPA suíça serão resolvidas pelos tribunais da Suíça. Um sujeito dos dados também pode abrir processos legais contra o exportador e/ou o importador de dados perante os tribunais da Suíça no local de sua residência habitual. As partes concordam em se submeter à jurisdição de tais tribunais."
- Até a entrada em vigor da DPA suíça, as Cláusulas P-C também protegerão dados pessoais de pessoas jurídicas, e as pessoas jurídicas receberão a mesma proteção sob as cláusulas P-C que as pessoas físicas.

Para os fins do DPA da Suíça, em que transferências de Dados Pessoais do Cliente sob o EULA estão exclusivamente sujeitas ao DPA da Suíça, as Cláusulas P-C, conforme aplicável de acordo com as Seções 8.1 e 8.2 deste DPA serão aplicadas com as seguintes emendas:

- Referências ao "Regulamento (UE) 2016/679" ou "àquele Regulamento" devem ser interpretadas como referências ao DPA da Suíça.
- Referências ao "Regulamento (UE) 2018/1725" são removidas.
- Referências a "União", "UE" e "Estado Membro da UE" devem ser interpretadas como significando a Suíça.
- A Cláusula 17 é substituída para declarar que "Estas Cláusulas são regidas pelas leis da Suíça".
- A Cláusula 18 é substituída para declarar:
"Qualquer disputa decorrente destas Cláusulas com relação à DPA suíça serão resolvidas pelos tribunais da Suíça. Um sujeito dos dados também pode abrir processos legais contra o exportador e/ou o importador de dados perante os tribunais da Suíça no local de sua residência habitual. As partes concordam em se submeter à jurisdição de tais tribunais."

- Até a entrada em vigor da DPA suíça, as Cláusulas P-C também protegerão dados pessoais de pessoas jurídicas, e as pessoas jurídicas receberão a mesma proteção sob as cláusulas P-C que as pessoas físicas.

Anexo C: Descrição da Transferência

Categorias de sujeitos dos dados cujos dados pessoais são transferidos:

Sujeitos dos dados incluem as pessoas sobre as quais os dados são fornecidos à Pix4D por meio de Ofertas Licenciadas por Você (ou por Sua instrução) ou por Usuários Autorizados, incluindo terceiros que aparecem no Conteúdo.

Categorias de dados pessoais transferidos:

Dados relacionados a pessoas fornecidos à Pix4D pelos Serviços por Você (ou por Sua instrução) ou por Usuários Autorizados, incluindo dados pessoais de terceiros que aparecem no Conteúdo.

Dados confidenciais transferidos (se aplicável) e restrições ou proteções aplicadas que levam totalmente em conta a natureza dos dados e os riscos envolvidos, como, por exemplo, limitação de finalidade estrita, restrições de acesso (incluindo acesso apenas para equipe que tenha feito treinamento especializado), manter um registro do acesso aos dados, restrições para transferências adiante ou medidas de segurança adicionais:

As partes não preveem a transferência de dados confidenciais.

A frequência da transferência (por exemplo, se os dados são transferidos uma só vez ou de modo contínuo):

Regular e contínua.

Natureza do processamento:

A Pix4D processará Dados Pessoais do Cliente para os fins de fornecer a Oferta Licenciada para uso por Você e os Usuários Autorizados de acordo com o EULA.

Propósitos da transferência de dados e processamento adicional:

O período para o qual os dados pessoais serão retidos ou, se isso não for possível, os critérios usados para determinar esse período:

O Prazo mais o período do fim do Prazo até a exclusão de todos os Dados do Cliente pela Pix4D conforme o EULA e este DPA.

Para transferências a (sub)processadores, especificar também o assunto, a natureza e a duração do processamento:

Consulte a lista de subprocessadores da Pix4D disponível em <https://www.pix4d.com/legal>.

Anexo D: Medidas de Segurança

A seguir está a descrição das medidas técnicas e organizacionais implementadas pela Pix4D (incluindo quaisquer certificações relevantes) para garantir um nível apropriado de segurança (as "**Medidas de Segurança**"), levando em conta a natureza, o escopo, o contexto e a finalidade do processamento, além dos riscos para os direitos e as liberdades dos sujeitos dos dados:

1. Medidas de pseudonimização e criptografia de dados pessoais
 - a) A pseudonimização é realizada de modo que nenhum dado seja combinado com um sujeito dos dados específico sem informações adicionais.
 - b) Informações adicionais para atribuir dados pessoais a um sujeito dos dados específico são mantidas em sistemas separados e seguros que estão acessíveis apenas por um número limitado de pessoas.
 - c) Ao criptografar dados pessoais, algoritmos e a extensão das chaves são mantidos proporcionais ao nível de confidencialidade dos dados.
 - d) Chaves de criptografia são mantidas seguras e são dadas apenas a um número limitado de pessoas.
 - e) Instrução interna garante que a anonimização/pseudonimização seja realizado quando possível no caso de divulgação ou mesmo depois do fim do período de exclusão estatutário.
2. Medidas para garantir a confidencialidade, a integridade, a disponibilidade e a resiliência contínuas dos sistemas e serviços de processamento
 - a) Um executivo de segurança ou membro designado da gerência sênior é indicado para ser responsável pela coordenação e o monitoramento das regras e dos procedimentos de segurança da informação.
 - b) Aspectos de proteção de dados são estabelecidos como uma parte integral da gestão de risco corporativo.
 - c) Planos de emergência e contingência são mantidos para as instalações em que os dados pessoais de sistemas de informação estão localizados.
 - d) Se necessário, uma avaliação de impacto da proteção dos dados (DPIA) é realizada.
 - e) A equipe é treinada e obrigada a manter confidencialidade e sigilo dos dados.
 - f) A equipe é informada sobre procedimentos de segurança relevantes e suas respectivas funções.
 - g) A equipe é informada sobre possíveis consequências de violar as regras e os procedimentos de segurança.
 - h) Instruções de trabalho sobre controle de acesso, segurança da comunicação e segurança operacional são fornecidas à equipe.
 - i) As instruções de trabalho descrevem explicitamente medidas de segurança, os procedimentos relevantes e as responsabilidades.
 - j) Todos os regulamentos, instruções e diretrizes de proteção de dados são documentados de modo central e ficam acessíveis a todos os funcionários.

- k) Componentes críticos para a operação do sistema são monitorados sempre e protegidos por sistemas de proteção na medida exigida para protegê-los contra incêndio, água, umidade, choques, calor, frio e falta de energia imprevista.
 - l) Componentes críticos para a operação do sistema podem ser substituídos dentro do período exigido no caso de colapso, por exemplo, por componentes reserva, sistemas RAID ou espelhamento de dados.
 - m) Quando necessário, são usadas partições separadas para operar sistemas e dados.
3. Medidas para garantir a capacidade de restaurar a disponibilidade e o acesso a dados pessoais de modo oportuno no caso de um incidente físico ou técnico
- a) Uma estratégia de backup é definida com base na quantidade de dados e sua frequência de mudança.
 - b) A estratégia de backup é projetada para recuperar dados pessoais para o último estado anterior à perda ou à destruição dos dados.
 - c) Sistemas de backup são fisicamente separados dos sistemas de produção.
 - d) As mesmas medidas de segurança são aplicadas aos servidores de backup e aos servidores de produção.
 - e) Pessoas encarregadas de restaurar dados são especialmente treinadas para essa tarefa.
4. Processos para teste, avaliação e análise regulares da eficácia de medidas técnicas e organizacionais para garantir a segurança do processamento (TOMS)
- a) A eficácia da TOMS é testada a intervalos predefinidos pelo "importador dos dados". A natureza e a frequência desses testes são definidas conforme a medida respectiva.
 - b) Medidas adequadas são definidas e adotadas se os testes mostram que as TOMS são insuficientes, não estão implementadas ou não demonstraram a eficácia necessária.
 - c) Novas TOMS são introduzidas se a revisão das TOMS atuais indicar que elas não são mais suficientes (por exemplo, novas ameaças).
 - d) Uma ou mais pessoa é designada para monitorar continuamente a eficácia das TOMS e coordenar testes e quaisquer medidas a serem adotadas.
5. Medidas para identificação e autorização do usuário
- a) O acesso a sistemas de informação é protegido por procedimentos de identificação e autenticação padrão do setor.
 - b) Dispositivos armazenamento de dados, estações de trabalho, notebooks, smartphones e tablets de são criptografados com métodos de criptografia padrão do setor.
 - c) Contas de usuário e permissões do usuário são gerenciadas por pessoas designadas (administradores).

- d) Os conceitos de autorização restritivos com base na necessidade dos direitos de banco de dados são gerenciados por um número mínimo de administradores.
 - e) O acesso a dados pessoais é restrito a funcionários que têm uma necessidade legítima de acessar esses dados pessoais dentro do escopo de sua função profissional ou cargo individual.
 - f) Dados coletados para fins diferentes podem ser processados separadamente dos demais dados.
 - g) Atividades do sistema além do acesso autorizado são impedidas.
 - h) São desenvolvidas e implementadas diretrizes sobre os seguintes tópicos: "senhas seguras", "exclusão/destruição", "mesa limpa", "dispositivo móvel".
 - i) Qualquer conta do usuário que permita autenticação é pessoal e usada por uma única pessoa.
 - j) A equipe é instruída a desabilitar sessões administrativas ao sair do local ou quando as estações de trabalho são deixadas desassistidas.
 - k) As senhas do usuário consistem em pelo menos oito caracteres, incluindo letras maiúsculas e minúsculas, dígitos e caracteres especiais.
 - l) Autenticação de dois fatores é usada para acessar sistemas críticos.
 - m) Um picador de arquivo e/ou destruição de arquivo externa cumpre o padrão de segurança DIN 66399.
6. Medidas para a proteção dos dados durante a transmissão
- a) O acesso remoto ocorre apenas por linhas criptografadas (VPN).
 - b) A transferência eletrônica de dados e a transmissão de dados pessoais são realizadas com métodos de criptografia padrão do setor. Para e-mails, pelo menos criptografia de linha (TLS) é usada, quando há suporte.
 - c) Procedimentos de assinatura são implementados quando necessário.
 - d) Os dados não são transferidos a terceiros desconhecidos.
7. Medidas para proteção de dados durante o armazenamento
- a) O acesso a dados específicos é restrito a quem precisa Processar esses dados. Isso é controlado por um modelo de autorização do usuário.
 - b) Quando relevante, diferentes dados do cliente são armazenados em diferentes bancos de dados.
 - c) Mídia de armazenamento externa que contém dados pessoais confidenciais é criptografada e protegida fisicamente
 - d) Direito de inserir, alterar e excluir dados atribuído com base em um conceito de autorização.
 - e) Direito de apagar é concedido de modo restrito.
8. Medidas para garantir a segurança física dos locais em que os dados pessoais são processados

- a) Sistemas e serviços são protegidos contra destruição ilegal ou acidental, perda acidental, alteração, acesso ou divulgação não autorizada.
 - b) Um sistema de alarme de roubo incluindo um alarme sempre ativo está instalado.
 - c) Portas externas e internas de estacionamento são protegidas com contatos de fechamento e magnéticos.
 - d) Chaves e cartões de chave são alocados a pessoas.
 - e) A entrada ou recepção tem alguém sempre durante o horário comercial.
 - f) Os prédios e as entradas estão sob constante vigilância por vídeo.
 - g) Visitantes sempre são acompanhados pelos funcionários.
 - h) Pessoal externo é cuidadosamente selecionado.
 - i) Para sistemas abrigados, hospedados e mantidos por prestadores de serviço externos, medidas correspondentes a serem implementadas e mantidas por esses prestadores de serviço foram providenciadas.
9. Medidas para garantir o registro do evento
- a) Autorizações de acesso e recuperação de dados são monitoradas e registradas.
 - b) A alocação de chaves e cartões de chave é registrada.
 - c) O acesso do visitante é registrado.
 - d) A entrada, a modificação e a exclusão de dados são registradas.
 - e) Esforços de restauração de dados são registrados.
 - f) Os resultados do teste de eficácia da TOMS agora são registrados.
 - g) Os resultados do teste da estrutura de relatório são registrados.
 - h) Incidentes de segurança e violações de dados são registrados. São mantidos registros que incluem a natureza da violação de dados, categorias e número aproximado de sujeito dos dados em questão, categorias e número aproximado de registros de dados pessoais em questão, período, consequências da violação de dados, procedimento para recuperar os dados, medidas adotadas para mitigar efeitos adversos, nomes das pessoas que relataram a violação de dados e nome das pessoas a quem a violação de dados foi relatada.
 - i) Registra a rastreabilidade dos usuários individuais, não de grupos de usuários.
10. Medidas para garantir a configuração do sistema, incluindo a configuração padrão
- a) Medidas técnicas adotadas para permitir que os sujeitos dos dados facilmente exerçam o direito de retirar o consentimento.
 - b) Configurações padrão amigáveis à proteção são usadas em software padrão e individual.

11. Medidas para TI interna e gerenciamento e governança de segurança de TI
 - a) Software antivírus e um firewall estão instalados em servidores e clientes para ajudar a evitar que software mal-intencionado obtenha acesso não autorizado aos sistemas.
 - b) Um sistema de detecção de invasão é implementado.
 - c) Um procedimento formalizado para lidar com incidentes de segurança está em vigor.
 - d) O acesso remoto por partes externas é monitorado.
 - e) O hardware e o software de TI são verificados a intervalos predefinidos para avaliar se precisam ser atualizados ou substituídos por questões de segurança.
12. Medidas para certificação/garantia de processos e produtos
 - a) A necessidade de certificações para sistemas e produtos é avaliada regularmente.
 - b) Certificações de segurança de dados (se houver) e auditorias (incluindo testes de penetração, conforme o caso) são repetidas regularmente.
13. Medidas para garantir a minimização de dados
 - a) Dados pessoais são coletados apenas na medida necessária para cumprir os fins pretendidos.
 - b) Dados pessoais mantidos são revisados periodicamente e excluídos se não são mais usados e nenhuma exigência legal ou contratual impede a exclusão de tais dados pessoais.
14. Medidas para garantir a qualidade dos dados
 - a) Quando adequado, a entrada de dados está sujeita a testes de plausibilidade.
 - b) Quando adequado, os usuários têm a oportunidade de verificar os dados inseridos.
15. Medidas para garantir a retenção de dados limitada
 - a) Quando adequado e possível, períodos de retenção são definidos.
 - b) Protocolos de arquivamento automatizados são usados para documentos e dados em sistemas produtivos, quando possível e apropriado.
16. Medidas para garantir a responsabilidade
 - a) Um processo formal é definido para acompanhamento de incidentes de segurança e violações de dados.
 - b) Mecanismos de controle relacionados à conformidade com os princípios de proteção de dados são baseados nos requisitos das leis de proteção de dados vigentes.

- c) Estruturas de relatório estão alinhadas com a organização do Grupo e a respectiva unidade e permitem reações dentro de um período razoável e, quando existir, legal.
- d) A eficácia das estruturas de relatório é testada a intervalos predefinidos.
- e) Medidas adequadas são definidas e adotadas se os testes mostram que as estruturas de relatório são insuficientes, não estão implementadas ou não têm a eficácia necessária.

17. Medidas para permitir a portabilidade de dados e garantir o apagamento

- a) Responsabilidades quanto à portabilidade dos dados são claramente definidas.
- b) Processos formalizados para solicitações de portabilidade de dados estão em vigor.
- c) Conjuntos de dados podem ser identificados e separados pelas funções de seleção do sistema empregado.
- d) Solicitações de portabilidade de dados são enviadas para as unidades corretas sem atraso e tratadas imediatamente de modo que os prazos estatutários sejam atendidos em qualquer caso.
- e) Medidas apropriadas são implementadas para garantir a remoção de dados pessoais dos sistemas do Provedor mediante o fim do Acordo Principal.
- f) Pessoas responsáveis pela portabilidade dos dados são treinadas e competentes em como lidar com solicitações sobre a portabilidade dos dados. Em particular, está claramente definido que informações devem ser divulgadas, transferidas ou excluídas e que solicitações ou partes das mesmas não devem ser cumpridas.
- g) Os dados pessoais são transmitidos em formatos estruturados, comumente usados e legíveis por máquina usando métodos seguros.