[Este modelo é publicamente compartilhado em <https://www.iubenda.com/pt-br/help/47355>]

# DPA - Modelo

### Contrato de Processamento de Dados (DPA)

nos termos do art. 28 do Regulamento Geral de Proteção de Dados (GDPR)

entre

 ................................................................................................

* + O Controlador

[se aplicável: Representante autorizado, conforme art. 27 do GDPR:

 ................................................................................................]

 .................................................................................................

* + O Processador

[se aplicável: Representante autorizado, conforme art. 27 do GDPR:

 ................................................................................................]

## 1. Objeto, prazo de vigência, dados pessoais processados e categorias dos titulares dos dados

(1) Objeto

* + O objeto deste DPA é a nomeação do Processador pelo Controlador e o fornecimento de instruções para o processamento de dados pessoais. As atividades de processamento que o Processador deve realizar são estritamente limitadas àquelas necessárias para o cumprimento do contrato principal assinado pelas partes em [*inserir a data*].

[*ou*

* + O Processador deve realizar as seguintes atividades de processamento em nome do Controlador:
	**..............................................................................................................**
	**..............................................................................................................**
	**..............................................................................................................**
	**..............................................................................................................**
	**..............................................................................................................]**

(2) Vigência

* + O prazo de vigência deste DPA corresponde ao prazo de vigência do contrato principal.

[*alternativamente:* especifique o prazo de vigência]

(3) Categorias de dados pessoais

* + As categorias de dados pessoais processados são:
		- informações pessoais identificáveis (por exemplo, nome, sobrenome, e-mail)
		- dados estatísticos ou outros dados de uso observados na internet (por exemplo, por meio de análises, serviços, etc.)
		- histórico do cliente
		- dados de cobrança, faturamento e pagamento
		- outros:….................................................. [*especifique de forma detalhada, principalmente se forem processados dados genéticos, biométricos ou outros dados confidenciais*]

(4) Categorias dos titulares dos dados

* + Os dados pessoais coletados e tratados estão relacionados a:
		- clientes
		- potenciais clientes
		- usuários de internet
		- funcionários, associados, membros da equipe
		- consultores internos
		- agentes autorizados
		- outros:….................................................. [*especifique*]

## 2. Transferência internacional de dados

(1) O Processador **compromete-se** a não transferir quaisquer dados pessoais para o exterior (*ou seja,* para fora do território do EEE) sem a autorização prévia por escrito do Controlador. Qualquer transferência internacional de dados e suas atividades de processamento serão realizadas em estrita conformidade com as instruções específicas e documentadas pelo Controlador.

*[opção 1 sem transferência de dados]*

(2) Ambas as partes estão cientes e acordam que as atividades de processamento de dados, nos termos deste contrato, não serão realizadas fora do EEE.

*[alternativamente, em caso de transferência internacional de dados]*

(2) Na data de assinatura do presente contrato, o Controlador toma ciência de que as seguintes atividades de processamento de dados, realizadas pelo Processador em seu nome, ocorrerão fora do EEE.

Tais atividades de processamento, especificamente autorizadas pelo Controlador, serão realizadas nos estados listados abaixo e em estrita observância às bases legais para transferência de dados estabelecidas nos artigos 45 e seguintes do GDPR, conforme aplicável a cada atividade de processamento.

|  |  |  |  |
| --- | --- | --- | --- |
|  | A | B | C |
| 1 | **país** | **atividade de processamento de dados** | **base legal para transferência** |
| 2 | *por exemplo, Suíça* | *por exemplo, serviço de hospedagem* | *por exemplo, juízo de adequação* |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |

(*As principais bases legais para transferência, de acordo com o GDPR, são:*

* + *um juízo de adequação proferido pela Comissão Europeia (artigo 45, parágrafo 3 do GDPR);*
	+ *normas corporativas vinculantes (artigo 46, parágrafo 2, alínea B, combinado com o artigo 47 do GDPR);*
	+ *Cláusulas-padrão contratuais (artigo 46, parágrafo 2, alíneas C e D do GDPR);*
	+ *Códigos de conduta (artigo 46, parágrafo 2, alínea E, combinado com o artigo 40 do GDPR);*
	+ *Processo de certificação. (artigo 46, parágrafo 2, alínea F, combinado com o artigo 42 do GDPR).*

*Para cada atividade de processamento elencada na tabela, selecione a respectiva opção na lista acima*)

## 3. Medidas técnicas e organizacionais

(1) Antes da celebração deste DPA, o Processador se compromete a adotar todas as medidas necessárias de segurança técnica e organizacional e a fornecer ao Controlador um documento com a descrição detalhada de tais medidas, também no que se refere especificamente ao presente contrato.

Tais medidas estão sujeitas à análise e aprovação prévia do Controlador.  Mediante a aprovação do Controlador, referidas medidas de segurança, documentadas como acima descrito, se tornarão parte integrante e substancial do presente contrato e serão incorporadas por referência. Na medida em que uma inspeção/auditoria realizada pelo Controlador revelar a necessidade de alterações, estas devem ser implementadas de comum acordo.

(2) O Processador declara que tomou todas as medidas de segurança de acordo com o artigo 28, parágrafo 3, alínea C e artigo 32 do GDPR, sobretudo combinado com o artigo 5, parágrafos 1 e 2 do GDPR. Tais medidas garantirão a segurança dos dados e um nível de proteção adequado ao risco de confidencialidade, integridade, disponibilidade e resiliência dos sistemas. De acordo com o artigo 32, parágrafo 1 do GDPR, o seguinte deve ser considerado ao avaliar a adequação das medidas de segurança adotadas: se as medidas podem ser consideradas de última geração, os custos de implementação, a natureza, o escopo e as finalidades do processamento, a probabilidade de violação de dados e a gravidade dos riscos para os direitos e liberdades das pessoas físicas.

 (3) As medidas técnicas e organizacionais estão sujeitas ao progresso e ao desenvolvimento técnico e tecnológico. Portanto, o Processador pode adotar medidas alternativas adequadas, que estejam atualizadas de acordo com a alteração do ambiente tecnológico. Ao fazê-lo, o nível de segurança do processamento não pode ser reduzido. Mudanças substanciais devem ser documentadas.

## 4. Direitos do titular dos dados

(1) O Processador compromete-se, na medida do possível, a cooperar e fornecer total assistência a fim de ajudar o Controlador a responder às solicitações dos titulares dos dados no que se refere ao exercício de seus direitos.

(2) Sobretudo, o Processador compromete-se a (**i**) comunicar imediatamente ao Controlador qualquer solicitação recebida pelos titulares dos dados sobre o exercício de seus direitos e, se viável e apropriado, (**ii**) permitir que o Controlador projete e implemente todas as medidas técnicas e organizacionais necessárias para responder às solicitações dos titulares dos dados.

(3) Não obstante o fato de o Controlador ser responsável por responder às solicitações dos titulares dos dados, o Processador pode aceitar ser encarregado pelo cumprimento de algumas solicitações específicas, desde que tais funções não exijam esforços desproporcionais do Processador e que os Controladores forneçam instruções detalhadas por escrito.

## 5. Outros deveres do Processador

Além de cumprir as disposições deste DPA, o Processador se compromete a cumprir todos os requisitos legais aplicáveis estabelecidos nos artigos 28 a 33 do GDPR. Para tanto, o Processador garante o cumprimento do que se segue:

* + **Nomeação de um Encarregado pelo tratamento de dados pessoais (DPO)**O atual DPO é:
	(INFORMAÇÕES COMPLETAS DO CONTATO)**....................................................................**
	**..............................................................................................................**
	**..............................................................................................................**O Processador deve informar imediatamente o Controlador sobre quaisquer alterações relacionadas ao DPO.

	[*ou* O Processador não é obrigado a nomear um DPO. O/A Sr./Sra. [*inserir nome, sobrenome, unidade organizacional, telefone, e-mail* ] é designado(a) como Pessoa de Contato em nome do Processador.]
	+ [→ escolha apenas se cabível] **Nomeação de um Representante** Visto que o Processador está estabelecido fora da UE e do EEE, este designou (INFORMAÇÕES COMPLETAS DO CONTATO)....................................................................
	**..............................................................................................................**
	**..............................................................................................................**como Representante na União, nos termos do artigo 27, parágrafo 1 do GDPR.
	+ **Confidencialidade**
	As atividades de processamento, nos termos deste DPA, devem ser realizadas apenas por indivíduos (como funcionários, agentes ou membros da equipe) que tenham sido instruídos pelo Processador sobre a maneira apropriada de processar dados, e que estejam contratualmente sujeitos à confidencialidade de acordo com o art. 28 parágrafo 3 (b) e art. 32 do GDPR.  O Processador, ou qualquer pessoa que atue sob sua autoridade e que tenha acesso aos dados pessoais, não processará esses dados, salvo sob instruções fornecidas pelo Controlador - incluindo os poderes concedidos sob esta DPA - a menos que seja obrigado a fazê-lo em virtude de lei.
	+ **Medidas Técnicas e Organizacionais**
	Implementação e cumprimento de todas as medidas técnicas e organizacionais adequadas no âmbito deste DPA, sobretudo, conforme estabelecido no art. 32 do GDPR. O Processador deve monitorar, de forma periódica, os processos internos e as medidas técnicas e organizacionais a fim de garantir que suas atividades de processamento sejam realizadas de acordo com os requisitos da lei de proteção de dados aplicável e com a proteção dos direitos dos titulares de dados. O Processador concederá a verificabilidade das medidas técnicas e organizacionais ao Controlador como parte dos poderes de supervisão mencionados na seção 7 deste contrato.
	+ **Cooperação com autoridades supervisoras**
	O Controlador e o Processador devem cooperar, mediante solicitação, com a autoridade supervisora. O Controlador deve ser imediatamente informado sobre quaisquer inspeções e medidas executadas pela autoridade supervisora, na medida em que estejam relacionadas às atividades deste DPA. Isso também se aplica caso o Processador esteja sendo investigado, ou seja parte de uma investigação por uma autoridade competente, por infrações a qualquer disposição relativa ao processamento de dados pessoais em conexão com o processamento deste DPA. Caso o Controlador seja objeto de inspeção por uma autoridade supervisora, multa administrativa, liminar, procedimento criminal, reclamação de responsabilidade por um titular dos dados, ou por um terceiro, ou qualquer outra reclamação relacionada ao processamento de dados realizado pelo Processador em razão deste DPA, o Processador envidará todos os esforços para auxiliar o Controlador.

## 6. Subprocessadores

(1) O Controlador autoriza o Processador a delegar aos subprocessadores parte das atividades de processamento, nos termos deste DPA. Os subprocessadores estarão, conforme exigido por lei, sujeitos às mesmas obrigações contratuais decorrentes deste contrato, nos termos do art. 28 parágrafo, 4 do GDPR.

[*o parágrafo (2) é opcional, somente se os subprocessadores já estiverem comissionados]*

(2) Na data de assinatura deste contrato, as partes tomam ciência e concordam que o Processador passa a comissionar, de forma contratual e nos termos do artigo 28, parágrafo 4 do GDPR, os seguintes subprocessadores:

|  |  |  |  |
| --- | --- | --- | --- |
|  | A | B | C |
| 1 | Subprocessador da empresa | Endereço/país | Atividade de processamento delegada |
| 2 |  |  |  |
| 3 |  |  |  |

(3) Fica entendido entre as partes que a comunicação de dados pessoais a qualquer subprocessador somente ocorrerá após o cumprimento de todas as condições estabelecidas no parágrafo (1) para a nomeação de subprocessadores.

(4) O Processador deve manter uma lista atualizada de subprocessadores. O Controlador será imediatamente notificado a respeito de qualquer alteração nessa lista, podendo se opor a tais alterações. Em caso de oposição, o Processador terá o direito de encerrar o vigente contrato com o Controlador, sem aviso prévio.
(5) O Processador assumirá, *perante* o Controlador, todas as responsabilidades e obrigações pelas atividades de seus subprocessadores.
(6) Caso um subprocessador preste serviços fora da UE/EEE, o Processador garantirá o cumprimento das regras relativas à transferência de dados para o exterior, conforme descrito na seção 2 deste DPA.

## 7. Auditorias

(1) O Controlador tem o direito de realizar inspeções ou de fazê-las por meio de um auditor escolhido conforme o caso. O auditor avaliará a conformidade do Processador com este DPA em suas operações comerciais por meio de verificações aleatórias, das quais o Processador será notificado com antecedência.
(2) O Processador permitirá que o Controlador verifique o cumprimento de suas obrigações, conforme previsto no artigo 28 do GDPR**.** Mediante solicitação, o Processador compromete-se a fornecer ao Controlador as informações necessárias e, principalmente, a demonstrar a implementação das medidas técnicas e organizacionais.
 (3) Evidências da implementação de tais medidas, que podem estar relacionadas não apenas às atividades deste DPA, também podem ser fornecidas por meio do

* + cumprimento dos Códigos de conduta aprovados nos termos do artigo 40 do GDPR;
	+ certificação conforme procedimento aprovado nos termos do artigo 42 do GDPR;
	+ certificados, relatórios ou extratos de relatórios do atual auditor fornecidos por órgãos independentes (por exemplo, auditor, DPO, departamento de segurança de TI, auditor de proteção de dados);
	+ uma certificação indicada por uma auditoria de segurança de TI ou de proteção de dados.

(4) O Processador poderá cobrar do Controlador uma taxa razoável para permitir inspeções.

## 8. Assistência ao Controlador

(1) O Processador deve ajudar o Controlador a cumprir as obrigações relativas à segurança de dados pessoais, aos relatórios de violações de dados, às avaliações de impacto de proteção de dados e às consultas prévias estabelecidas nos artigos 32 a 36 do GDPR, incluindo

* a garantia das normas de proteção adequadas através de medidas técnicas e organizacionais, considerando o tipo, as circunstâncias e as finalidades do processamento, a probabilidade de violação de dados e a gravidade de possíveis riscos para as pessoas físicas
* a garantia da detecção imediata de infrações
* a comunicação imediata sobre violações de dados ao Controlador
* a assistência ao Controlador na resposta às solicitações dos titulares dos dados para o exercício de seus direitos

(2) O Processador poderá cobrar do Controlador uma taxa razoável por serviços de assistência que não estejam incluídos na descrição dos serviços, o que não será considerado conduta imprópria, falta ou infração.

## 9. Poderes diretivos do Controlador

(1) O Processador não processará nenhum dado pessoal decorrente deste DPA, exceto nas instruções documentadas pelo Controlador, salvo se exigido pela legislação da União ou do Estado Membro.
(2) Caso o Controlador exija qualquer alteração no processamento de dados pessoais estabelecido pelas instruções documentadas mencionadas na seção 2, o Processador informará imediatamente o Controlador se considerar que tais alterações podem resultar em violações às disposições de proteção de dados. O Processador pode abster-se de realizar qualquer atividade que possa resultar em tal violação.

## 10. Responsabilidade

(1) As partes deste DPA se obrigam a indenizar a parte contrária por danos ou despesas resultantes da violação culposa deste DPA, incluindo qualquer violação culposa cometida por seu representante legal, subcontratados, funcionários ou quaisquer outros agentes. Ademais, as partes se obrigam a indenizar a parte contrária por qualquer reclamação de terceiros relacionada à sua violação culposa.
 (2) O art. 82 do GDPR permanece inalterado.

## 11. Exclusão e devolução de dados pessoais

(1) O Processador não criará cópias ou duplicatas dos dados sem o conhecimento e consentimento do Controlador, exceto cópias de backup, na medida em que sejam necessárias para garantir que os dados sejam processados corretamente, e quando a retenção de tais dados for exigida por lei.
(2) Após a conclusão da prestação de serviços, o Processador deverá, à escolha do Controlador, excluir de maneira compatível com a proteção de dados ou devolver ao Controlador todos os dados pessoais coletados e processados ao abrigo deste DPA, salvo se alguma disposição legal aplicável exigir armazenamento adicional dos dados pessoais.

(3) No entanto, após o encerramento do contrato, o Processador poderá reter todas as informações necessárias para demonstrar a conformidade das atividades de processamento realizadas.
(4) A documentação supramencionada na alínea (3) deve ser armazenada pelo Processador de acordo com os períodos de retenção aplicáveis, previstos em lei ou fixados de qualquer forma. O Processador poderá entregar a documentação ao Controlador após o término do contrato. Nesse caso, o Processador fica isento da obrigação de manter tal documentação.