



Política de Privacidade de Dados



O que são Dados Pessoais?

São todas as informações que podem identificar uma pessoa natural, por exemplo:

CPF
RG
Telefone
Endereço
Origem racial ou étnica
Religião
Filiação política
Dado referente à saúde



Dados sensíveis

Este documento define os **princípios que regem o Tratamento de Dados Pessoais da Astellas**, em todos os países em que ela atua.

Nós sabemos como, para as pessoas, a privacidade de seus dados pessoais é muito importante e temos como objetivo agir de maneira ética, transparente e em conformidade com toda legislação nacional e internacional de privacidade e proteção de dados.



A quem se aplica esta Política?

A todos que compõem a Astellas: nossos conselheiros, diretores, colaboradores, terceiros. Também àqueles que tratam Dados Pessoais para nós ou em nosso nome, uma pessoa natural, por exemplo:

Qualquer operação com Dados Pessoais, desde a coleta até a eliminação

Os 6 princípios básicos do nosso Tratamento de Dados Pessoais



Tratamento lícito, justo e transparente

Coletamos dados apenas para fins específicos e legítimos

Dados adequados e relevantes

Mantemos os dados seguros e protegidos de perdas e vazamentos

Dados precisos e atualizados

Guardamos os dados só pelo tempo necessário

Como cuidamos dos dados pessoais em cada passo do caminho

1 – A coleta

Em algum momento do trabalho, você poderá se deparar com a necessidade de coletar dados pessoais, seja de colaboradores, parceiros ou clientes.

Essa coleta precisará seguir algumas diretrizes:

- ser feita em conformidade com a **legislação** e com esta Política;
- ser conduzida de maneira **justa** e transparente;
- ser **reduzida ao mínimo necessário** de dados para atingir seu propósito;
- contar com uma **base legal**

O que devemos nos perguntar nesse momento?

1. Quais dados eu realmente preciso para atingir meu objetivo?
2. Meu objetivo é justo? E lícito?
3. Como farei para que a coleta desses dados seja feita de forma transparente?

As **bases legais** são as situações que justificam e permitem que seja feito um tratamento de dados. A Lei Geral de Proteção de Dados (LGPD) elenca as seguintes bases:

- para cumprir obrigações legais ou regulatórias;
- para realizar pesquisas através de órgãos públicos ou implementar políticas públicas;
- para executar um contrato;
- para exercer um direito;
- para proteger a vida e a saúde;
- para proteção ao crédito;
- por legítimo interesse;
- a pessoa deu o seu consentimento.

Sobre CONSENTIMENTO

Obtenha consentimento sempre que você for usar dados pessoais (por exemplo, para o envio de mensagens) ou quando planejar coletar dados sigilosos.

Quando a base do tratamento de dados for o consentimento, é necessário dar ao **Titular** dos dados a possibilidade de revogar o seu consentimento a qualquer hora.

Pessoa a quem se referem os dados



Garantindo a TRANSPARÊNCIA

Quando exigido por lei, forneça um Aviso de Privacidade no momento de coletar os dados, explicando o porquê da coleta, como será o tratamento, para quem as informações poderão ser enviadas.



Trabalhe em parceria com o nosso **Escritório de Privacidade de Ética e Compliance** para trazer esta Política para a sua realidade.

Você deve procurá-los:

- Para conhecer as exigências locais e entender se será necessário obter o consentimento;
- Para saber se precisará oferecer um Aviso de Privacidade e como fazer isso;
- Antes de implementar novos sistemas, projetos e relações comerciais que envolvam tratamento de Dados Pessoais.

Mudando a forma de pensar a proteção de dados

Traga a Proteção de Dados para o centro da discussão já no momento de **desenvolvimento** de um novo projeto, sistema ou relação comercial, em como garantir a conformidade com as leis.

2 – O uso

Os dados pessoais deverão ser usados sempre de uma maneira legítima e apenas para a **finalidade** para a qual foram coletados.

Motivo do uso dos dados.

Deve ser legítima, específica, explícita e informada ao Titular

Seu uso deve responder a alguns princípios básicos:

- Caso haja a necessidade de **consentimento**, é preciso obtê-lo antes de fazer qualquer uso dos Dados;
- O acesso aos Dados deverá ficar **restrito** ao menor número de pessoas necessário e deve ser concedido de forma documentada;
- Devem ser mantidos **corretos** e **atualizados**.

O que devemos nos perguntar nesse momento?

1. Que pessoas realmente precisam ter acesso a esses dados?
2. Tenho uma necessidade comercial legítima para usá-los?
3. Preciso de consentimento para isso? Eu tenho esse consentimento?
4. Como farei para manter os dados precisos e atualizados?

Para garantir a segurança e o bom uso dos dados pessoais, contamos com alguns mecanismos:



Obrigatório em regulamentos de privacidade de dados em muitos países.

ROPA (Records of Processing Activities), ou Registro de Atividades de Processamento

É um levantamento de todos os processos de negócios que usam informações pessoais na Astellas. Para isso, o ROPA considera informações sobre:

- Os **processos de negócios** da Astellas que promovem ou fazem uso de informações pessoais;
- Os **tipos de informações** pessoais envolvidas;
- Os **tipos de pessoas** que têm os dados processados; e
- Os **sistemas e ferramentas** usados no processamento.

PIA (Privacy Impact Assessment), ou Avaliação de Impacto de Privacidade

É um método usado para identificar, avaliar e tratar os riscos de privacidade que ocorrem no processamento de dados pessoais. Nesse sentido, o Gestor de Projeto deve:

- Antes do processamento, **solicitar e obter a aprovação de uma PIA** como parte do processo de planejamento da iniciativa.
- Se a metodologia do processamento de informações pessoais for alterada após a aprovação de uma PIA, **realizar a atualização dessa atividade de processamento**.

Uso de dados para uma NOVA FINALIDADE

Caso surja uma nova finalidade para o uso de algum Dado Pessoal **que não tenha sido identificada e informada na fase de coleta**, avalie cuidadosamente a situação.

Ela precisará de uma nova base legal.

Além disso, considere a possibilidade de notificar os Titulares desses dados ou mesmo de obter o consentimento específico deles para essa nova finalidade.

A possibilidade de tornar os dados ANÔNIMOS

Quando, para o uso dos dados, não for necessário saber a identidade do Titular, eles deverão ser desidentificados.

Isso é feito em um processo de pseudonimização ou de anonimização, o que irá impedir que o Titular seja associado àqueles Dados.

Esse procedimento irá nos proteger de eventuais incidentes.

Cuidados especiais para Dados Pessoais especiais

Dados Pessoais Sensíveis

Dados Pessoais que podem causar um maior dano ao Titular em caso de vazamentos, principalmente por conta do potencial discriminatório.

- As **bases legais** são limitadas.
- Caso seja necessário o **consentimento**, ele deve ser específico e estar em destaque.

Tomar cuidado com dados que não são, eles mesmo, Sensíveis, mas que podem indicar um Dado Sensível (ex. compras em farmácia podem indicar informações de saúde)



Em caso dúvida, procure o
Encarregado de Privacidade de Dados.

Dados pessoais de crianças e adolescentes (menores de 18 anos)

- Devem ser tratados sempre considerando o “melhor interesse” do menor, ou seja, com a finalidade de **beneficiá-lo**, mesmo que indiretamente.
- Na maioria dos casos, é necessário o consentimento do responsável legal.)



Se certificar que o tratamento está em
conformidade com a legislação local.



Mantendo os dados em segurança

Um dos nossos grandes objetivos é proteger os Dados Pessoais de **Incidentes de Segurança**, ou **DPI (Data Privacy Incident)**

Qualquer incidente que ameace a confidencialidade, integridade ou dispositivos de segurança dos sistemas de informação da Astellas e/ou das redes que fornecem as informações, bem como violações das políticas de segurança.

Exemplos de incidentes:

- perda ou roubo de aparelhos e dispositivos;
- acesso, uso, divulgação, alteração ou destruição não autorizados;
- ransomware ou malware;
- phishing, vishing ou smishing.

Por isso é importante **cumprir as políticas e procedimentos** de negócios, Sistemas de Informação (SI) e segurança da Astellas.



Nos ajude a manter os dados pessoais seguros, tendo cautela com divulgações inadvertidas:

Não discuta essas informações em locais públicos ou redes sociais.

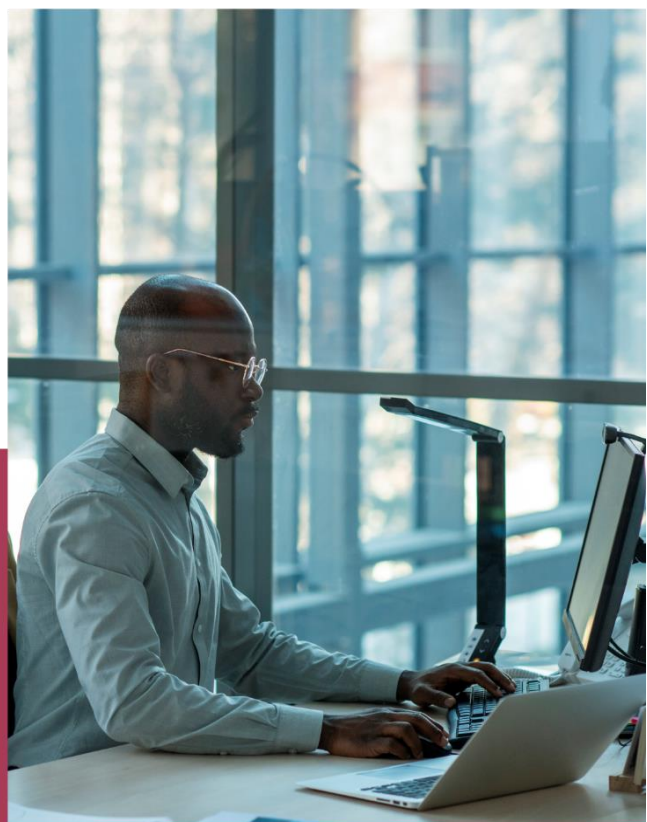


Não responda ligações ou e-mails sobre dados pessoais com pessoas não solicitadas.



Caso você tenha conhecimento de qualquer caso concreto ou suspeita dessas práticas, **informe imediatamente** o Escritório de Privacidade do Departamento de Ética e Compliance, em **br.privacidade@astellas.com**.

(Consulte o SOP-1712 Gestão de Incidentes de Privacidade de Dados para mais detalhes.)



O envio de dados pessoais

Para dentro e fora da Astellas

- Só poderá acontecer se houver um **objetivo comercial legítimo** para a transferência.
- Deve ser feito de maneira **segura e compatível com o grau de risco**. É recomendado o uso de ferramentas de transferência de arquivo aprovadas ou criptografia.
- Os **padrões e controles de privacidade de Dados do terceiro devem ser adequados**. Além disso, é possível fazer restrições de uso e acordos contratuais.

Para fora do país

Quando a lei exigir, será necessário:

- Obter consentimento dos Titulares para a transferência internacional de seus dados.
- Restringir ou implementar as cláusulas contratuais necessárias.

Em determinadas jurisdições, a transferência de Dados Pessoais entre países só é permitida após avaliações adicionais, de acordo com os processos e procedimentos relevantes definidos pela Astellas.

Consulte o Escritório de Privacidade em caso de dúvidas.

Garantindo os DIREITOS DOS TITULARES



Caso o Titular envie uma pergunta ou solicitação relacionada aos seus dados pessoais, responda prontamente.

Os Titulares podem enviar uma **DSR** (Data Subject Right) para:

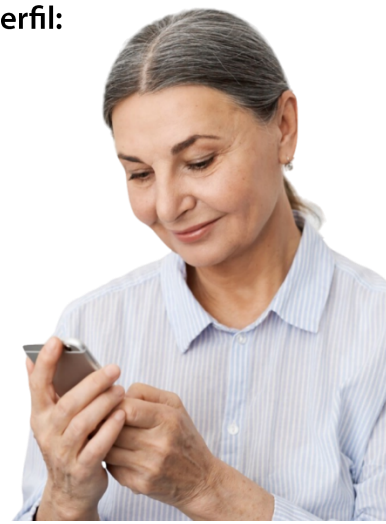
Solicitação ou consulta de qualquer indivíduo para exercer os seus direitos à privacidade.

- **Acessar:** forneça os dados tratados
- **Excluir:** remova os dados e interrompa o tratamento
- **Corrigir:** corrija dados imprecisos ou incompletos
- **Restringir:** limite o tratamento
- **Pedir a portabilidade:** forneça os dados em um formato em que possam ser reutilizados
- **Fazer uma objeção:** interrompa o tratamento para determinadas finalidades ou circunstâncias
- **Se opor a processos automáticos de tomada de decisão ou elaboração de perfil:** deixar de usar os dados quando isso foi feito com base somente em processos automáticos.

3 – A retenção de dados pessoais

Mesmo após atingir a finalidade para a qual foram coletados, é possível que ainda seja necessário manter os dados pessoais. Mas, lembre-se: isso deve ser feito apenas pelo tempo necessário para atender a requisitos comerciais ou legais.

Consulte o STL-3246, Prazo de Retenção dos Registros da Astellas.



Saiba mais sobre esta Política

Relate violações

Nós **investigaremos qualquer relato** de tratamento inadequado de dados pessoais. As violações a esta Política podem levar a **medidas disciplinares**, inclusive demissões.

Entre em contato com o Escritório de Privacidade ou envie uma comunicação ao **Departamento de Ética e Compliance pelo EthicsPoint.**



www.astellas.ethicspoint.com

Nós não toleraremos retaliações contra aqueles que denunciam violações

Quem é quem na proteção de dados

Diretor de Ética & Compliance:

- Responsável por qualquer alteração ou suspensão desta Política. Deve aprovar toda revisão feita.
- Aprova as medidas que forem avaliadas como de mais alto risco.

Comitê de Privacidade:

Trabalha pelo engajamento dos principais parceiros da Companhia que podem ser impactados pela Política.

Encarregado:

Principal responsável pela gestão do Programa de Privacidade e ponto de contato entre nós, Autoridades Públicas e os titulares.

Escritório de Privacidade:

Está pronto para tirar suas dúvidas. Entre em contato por **dpi@astellas.com**.



