



## **POLÍTICA INTERNA DE PRIVACIDADE E PROTEÇÃO DE DADOS**

*Diretrizes para tratamento interno de dados pessoais no Instituto Rede Jubileu Sul/Brasil*

A Política Interna de Privacidade e Proteção de Dados (“Política”) estabelece padrões e orienta o Tratamento de Dados pessoais realizado em nome do Instituto Rede Jubileu Sul/Brasil por seus Colaboradores.

### **1. A quem se aplica**

Esta Política destina-se às pessoas que trabalham ou prestam serviços junto ao Instituto Rede Jubileu Sul/Brasil (“Jubileu Sul Brasil”), assim como àquelas que integram as organizações, coletivos e movimentos sociais da Rede Jubileu Sul (“Colaboradores”) e que lidam com dados pessoais. É um dever do Jubileu Sul Brasil e de cada um de seus Colaboradores que realizar Tratamento de Dados Pessoais observar os termos desta Política.

São considerados “dados pessoais” os dados relacionados a uma pessoa natural, também chamada de pessoa física, que permita a sua identificação. Você aprenderá mais sobre isso nas próximas páginas. Além disso, ao final da presente Política, há um Glossário de todos os termos-chaves utilizados (**Anexo I**).

### **2. Objetivos**

Os objetivos desta Política são:

- (a)** Gerar compreensão a todos os Colaboradores do Jubileu Sul Brasil de que dados pessoais são uma extensão da personalidade dos indivíduos e que cuidados específicos devem ser adotados;
- (b)** Oferecer conhecimento e diretrizes aos Colaboradores do Jubileu Sul Brasil para que realizem o tratamento dos dados pessoais de maneira adequada;
- (c)** Construir fluxos internos capazes de fornecer aos titulares de dados pessoais parceiros do Jubileu Sul Brasil e ao público em geral informações precisas sobre como os seus dados são tratados, retidos e eliminados;
- (d)** Contribuir para o cumprimento pelo Jubileu Sul Brasil da Lei Geral de Proteção de Dados, normas relacionadas e boas práticas do setor.

Se encontrar dificuldade na aplicação dessa política ou tenha qualquer dúvida, pode escrever para o e-mail [encarregadodedados@jubileusul.org.br](mailto:encarregadodedados@jubileusul.org.br).

### **3. Time de Privacidade e Proteção de Dados do Jubileu Sul Brasil**

- Encarregada de Dados (DPO): **Rosilene Wansetto** | e-mail: [encarregadodedados@jubileusul.org.br](mailto:encarregadodedados@jubileusul.org.br)



- Substituta da Encarregada de Dados: **Lucimeire Araujo de Souza Paludette** | e-mail: encarregadodedados@jubileusul.org.br

#### **4. Passos dados pelo Jubileu Sul Brasil em direção à adequação à LGPD**

- Relatório de diagnóstico de conformidade e indicação de medidas de adequação (feito)
- Mapeamento de fluxo de dados da organização (feito)
- Revisão de Aviso de Privacidade e da política de cookies, disponibilizados no site oficial do Jubileu Sul Brasil, como política de privacidade externa (<http://jubileusul.org.br/pdfs/lgpd.pdf>)
- Aprovação de Política Interna de Privacidade e Proteção de Dados (presente documento)



## SUMÁRIO

I. “Privacy by Design”: a Privacidade e a preocupação com a Proteção de Dados desde o início .....	4
II. O Ciclo de vida de um Dado Pessoal.....	5
III. Como coletar o dado pessoal? .....	6
IV. Como Tratar dados pessoais? .....	9
V. Como compartilhar dados pessoais?.....	11
VI. O Armazenamento e a Retenção dos dados pessoais .....	13
VII. Como eliminar dados pessoais? .....	14
VIII. A Encarregada de Dados.....	15
IX. Violação de Dados e Incidentes de Segurança .....	17
X. Violação à Política .....	21



## I. “PRIVACY BY DESIGN”: A PRIVACIDADE E A PREOCUPAÇÃO COM A PROTEÇÃO DE DADOS DESDE O INÍCIO

A expressão “*privacy by design*” consiste na proposta de incorporar o zelo com a privacidade e a proteção de dados pessoais desde o início de qualquer projeto ou atividade do Jubileu Sul Brasil, de forma que sejam pensadas e adotadas medidas focadas no cumprimento da LGPD, evitando a necessidade de sua reestruturação completa posteriormente.

**IMPORTANTE!** Durante todo o processo de idealização de projetos e atividades, a Encarregada de Dados deve ser envolvido nos debates.

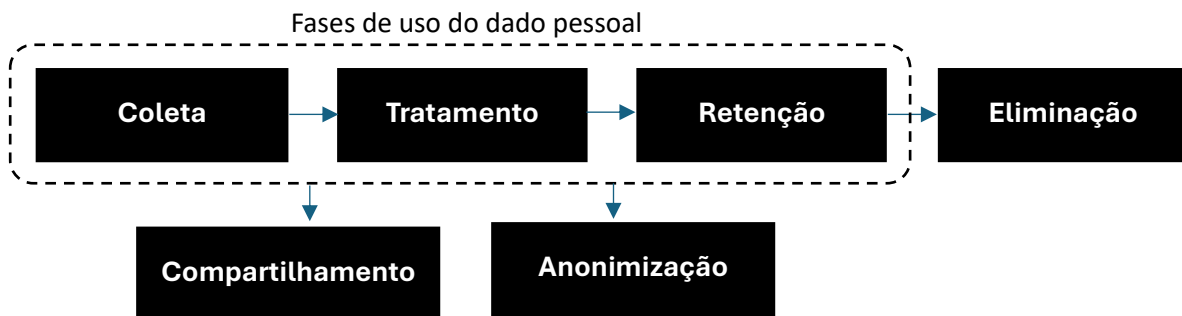
Como princípios para promover a privacidade desde o início, destacam-se:

<b>1</b>	<b>Atuação preventiva e não reativa:</b> As atividades e os projetos que envolvem dados pessoais devem ser organizados e estruturados de forma a evitar práticas de desvio de finalidade, compartilhamento inseguro e outros tipos de conduta que podem colocar em risco os titulares de dados pessoais.
Na prática: Oriente constantemente os colaboradores que estão trabalhando em cada projeto ou atividade, sobre como os dados pessoais devem ser tratados, de acordo com esta política e a política de privacidade externa do Jubileu Sul Brasil.	
<b>2</b>	<b>Privacidade como padrão:</b> Significa efetivar os princípios da LGPD garantindo que apenas o mínimo necessário de dados dos titulares seja utilizado para atingir o resultado de projeto ou atividade do Jubileu Sul Brasil.
Na prática: Seguir as disposições desta política sobre a estruturação do ciclo de vida dos dados pessoais e as medidas que devem ser adotadas.	
<b>3</b>	<b>Funcionalidade total:</b> Normalmente, a ideia de garantia de privacidade é atrelada à perda de algum tipo de funcionalidade, de possibilidade de pesquisa, ou de benefício. A ideia atrelada à aplicação deste princípio é balancear a privacidade do beneficiário das atividades ou dos projetos (e titulares de dados pessoais) sem perda ao Jubileu Sul Brasil em razão da garantia deste direito.
Na prática: Deve-se levar em consideração na construção do projeto ou planejamento da atividade, a harmonia entre os interesses do Jubileu Sul Brasil e os direitos do titular de dados pessoais, buscando-se gerenciar de forma responsável o possível impacto que as escolhas podem trazer aos titulares de dados pessoais.	

<b>4</b>	<b>Segurança de ponta a ponta durante o ciclo de vida dos dados:</b> Análise prévia considerando o trajeto dos dados, a respeito de quais medidas técnicas (TI) e administrativas podem ser adotadas para garantir a segurança dos dados dentro das atividades.
----------	---

## II. O CICLO DE VIDA DE UM DADO PESSOAL

"Ciclo de vida" significa que os dados pessoais possuem um caminho a ser seguido desde o momento que entram no Jubileu Sul Brasil até a eliminação definitiva. Cada uma das etapas descritas no fluxograma a seguir corresponde às categorias de tratamento desde a captação do dado pessoal. Para que o gerenciamento deste ciclo possa ser realizado, existem processos e registros que solicitamos para você, Colaborador, seguir e/ou auxiliar seu gestor.



**Coleta:** é o primeiro contato do Jubileu Sul Brasil com o dado pessoal independentemente do meio utilizado para a recepção do dado, podendo ser compartilhado pelo próprio titular de dados pessoais ou por terceiros.

**Tratamento:** envolverá qualquer operação de classificação, armazenamento, utilização, reprodução, processamento, avaliação ou controle da informação, extração ou modificação do dado pessoal. O tratamento é guiado conforme as finalidades e necessidades sinalizadas ao titular de dados pessoais nos termos de consentimento e/ou políticas de privacidade, a depender da base legal aplicável.

**Retenção:** está etapa se inicia quando está finalizada a finalidade de tratamento da informação e há a necessidade de armazenamento do dado pessoal. A depender do dado pessoal e do fundamento legal para sua retenção pelo Jubileu Sul Brasil, os prazos máximos para sua retenção podem variar (conforme **Anexo III**).

**Eliminação:** encerrado o período de retenção aplicável, o dado pessoal precisará ser eliminado de maneira correta, de forma que ele não possa ser mais recuperado e acessado pelo Jubileu Sul Brasil.

**Compartilhamento:** envolverá qualquer operação de transmissão, distribuição, comunicação, transferência, difusão ou compartilhamento do dado pessoal pelo Jubileu Sul Brasil a outros agentes de tratamento.

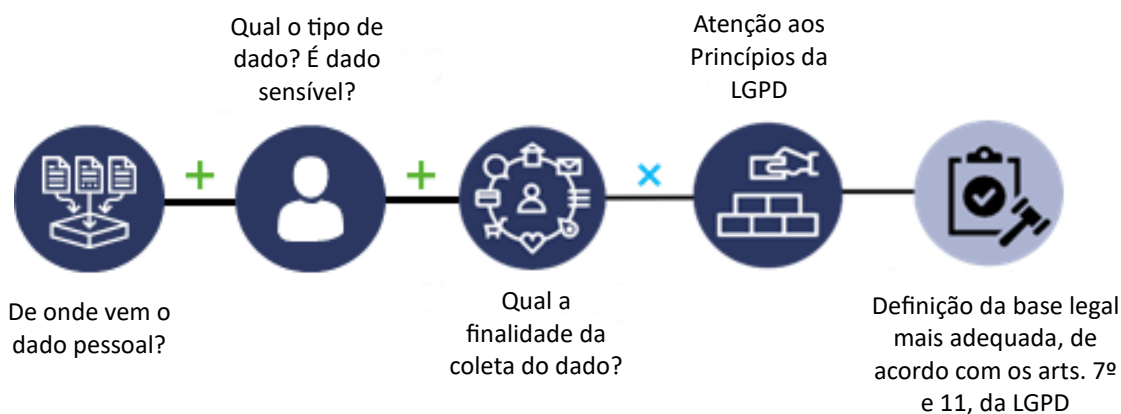
**Anonimização:** processo pelo qual se perde a capacidade de identificar o titular de dados pessoais a determinado dado pessoal se refere, podendo ocorrer de forma irreversível (anonimização) ou reversível (pseudonimização).

### III. COMO COLETAR O DADO PESSOAL?

A coleta é o primeiro contato que o Jubileu Sul Brasil terá com o dado pessoal. Assim, os Colaboradores devem seguir os seguintes passos para atender à LGPD:

#### 1. Determinar a base legal para o tratamento dos dados pessoais

- Antes de iniciar a coleta de dados pessoais, é necessário estruturar a atividade de acordo com a lógica do “privacy by design”. Ou seja, deve-se entender os dados efetivamente necessários, e, na sequência, determinar uma base legal para a coleta dos dados de acordo com a finalidade pretendida.



**ATENÇÃO!** A definição de qual base legal será utilizada na atividade de tratamento é feita pela DPO do Jubileu Sul Brasil! É importante que você, Colaborador, entenda o fluxo de análise para que possa fornecer as informações que ele precisar para determinar a base legal.



## 2. Inserir avisos de privacidade e política de privacidade no local de coleta de dados

- Todas as vezes que forem disponibilizados meios para que os titulares de dados possam inserir dados pessoais (como em formulários online, etc), deve constar um “aviso de privacidade” – ou seja, um comunicado que dá transparência para os titulares sobre como trataremos no Jubileu Sul Brasil os dados que eles estão nos fornecendo.
- Este aviso deve refletir a realidade do tratamento de dados pessoais que será feito pelo Jubileu Sul Brasil. Abaixo, compartilhamos um exemplo que deve ser adaptado junto com a Encarregada de Dados, de acordo com cada atividade ou projeto a ser desenvolvido pelo Jubileu Sul Brasil.

*“Os dados pessoais de [inserir os dados pessoais coletados na atividade] coletados nessa atividade são utilizados para [inserir as atividades para as quais os dados pessoais serão utilizados, por exemplo: inscrição, triagem, pesquisa, prestação de contas, deixar claro para o titular se houver mais de uma finalidade].*

*Para atingir essa(s) finalidade(s), o Jubileu Sul Brasil pode compartilhar os dados pessoais com [inserir compartilhamento de dados pessoais com parceiros, financiadores, empresas que viabilizam a atividade, conforme o caso], que auxiliam a organização a viabilizar a atividade oferecida para você. Os dados serão mantidos durante [inserir a estimativa temporal de manutenção dos dados se o titular não requisitar a eliminação].*

*“Para mais informações, consulte nossa Política de Privacidade ou, caso deseje exercer seus direitos como titular de dados, você pode nos contatar por meio do endereço eletrônico: <<[encarregadodedados@jubileusul.org.br](mailto:encarregadodedados@jubileusul.org.br)>>.”*

## 3. Coletando corretamente o Consentimento (se aplicável)

- Quando a base legal definida na etapa 1 for o Consentimento, deve-se ter especial atenção sobre a manifestação do titular. Para a lei, a coleta correta do consentimento deve ser:

<i>[No caso de tratamento de <b>Dados Pessoais</b>]</i>		
O Aviso de Privacidade deve conter informações <b>claras e inequívocas</b> sobre o tratamento	<b>+</b>	O Consentimento deve ser uma <b>manifestação livre</b> do titular de <b>sua concordância</b>
Desta forma, quando a base legal for o Consentimento, no momento da coleta de dados pessoais, deve existir uma caixa de seleção ( <i>checkbox</i> ) para que o titular expresse efetivamente sua vontade		
Exemplo de caixa de seleção selecionável para tratamento de dados pessoais:		



<input type="checkbox"/>	<b>Concordo</b> com o tratamento desses dados pessoais para a finalidade de <<inserir finalidade>> pelo Jubileu Sul Brasil
--------------------------	--

[No caso de tratamento de <b>Dados Pessoais Sensíveis</b> ]		
O Aviso de Privacidade deve conter informações <b>específicas, claras e inequívocas</b> sobre o tratamento	+	O Consentimento deve ser uma <b>manifestação livre</b> do titular de <b>sua concordância</b>
No caso de dados pessoais sensíveis, portanto, é importante que o Aviso de Privacidade também seja específico, indicando exatamente qual dado sensível será coletado e qual a necessidade relacionada para sua coleta.		
A) Quando existir a coleta de dado pessoal sensível, <u>mas ele não for efetivamente necessário</u> para a execução da atividade, deve-se realizar a coleta da seguinte forma, inserindo a opção para o titular que prefira não informar o dado sensível em questão. Exemplo:		
<input type="checkbox"/>	<i>Prefiro <b>não</b> responder</i>	<input type="checkbox"/> <b>Concordo</b> expressamente com o uso desses dados para a finalidade de <<inserir finalidade>> pelo Jubileu Sul Brasil.
B) Quando o tratamento de dados pessoais sensíveis for <u>indispensável</u> , a coleta do Consentimento deve ser realizada conforme exemplo abaixo:		
<i>Tratamento de dados pessoais sensíveis</i>		
<i>Para esta atividade, será necessário o tratamento de alguns dados pessoais sensíveis, tais como raça e origem étnica,</i>		
<i>Marque abaixo uma das opções a seguir:</i>		
<input type="checkbox"/>	<b>Concorda expressamente</b> com o uso desses dados para a <<inserir finalidade>> pelo Jubileu Sul Brasil.	
<input type="checkbox"/>	<b>Não concorda</b> com o tratamento dos seus dados pessoais sensíveis, entendendo que a recusa do tratamento destes dados <u>inviabilizará</u> a sua participação na atividade.	

#### 4. Recebendo dados pessoais por e-mail (se aplicável)

- É comum que na comunicação por e-mail tanto entre a equipe interna quanto na comunicação com terceiros, ocorra coleta de dados pessoais. Por diversas vezes, recebemos estas informações para contratação, inscrição, tirar dúvidas, responder solicitações e comunicações, dentre outras atividades.
- Assim, a **primeira instrução** é a adoção da confidencialidade como padrão para todos os e-mails. A seguir, você encontra o passo a passo para habilitar esta função: [Gmail](#) e [Outlook](#).





- A **segunda instrução** consiste em realizar o *backup* dos dados pessoais e documentos compartilhados por e-mail para o armazenamento interno do Jubileu Sul Brasil. A seguir, você encontra as instruções para realização do *backup* de forma correta: [Gmail](#) e [Outlook](#).

#### IV. COMO TRATAR DADOS PESSOAIS?

A partir da entrada do dado pessoal no Jubileu Sul Brasil, ele precisará ser armazenado corretamente. O armazenamento consiste no ato de salvar ou guardar as informações. Para este processo em específico, é necessário observar algumas medidas que, sendo implementadas, dão maior segurança para os dados pessoais.

- Medidas administrativas individuais: na sua atividade diária, Colaborador, você deve seguir as seguintes medidas para garantia da segurança das informações, além daquelas indicadas no guia “Boas práticas em Segurança Digital” do Jubileu Sul Brasil:
  - Quando se ausentar de sua estação de trabalho ou da vista da sua máquina, você deve suspender o sistema para que os dados não fiquem expostos;
  - Quando você encerrar o dia de trabalho deve realizar o *logoff* (desconectar) dos sistemas do Jubileu Sul Brasil: e-mail e sistemas de armazenamento. Não habilite o *log-in* automático nestes sistemas! Insira sua credencial de identificação e senha sempre que iniciar o dia ou quando ausentar-se por muito tempo do seu local de trabalho;
  - Não utilize informações pessoais na criação/alteração de suas senhas ou padrões comuns e fracos.
- Medidas de integridade controladas pela administração do Jubileu Sul Brasil: a Diretoria do Jubileu Sul Brasil, em conjunto com a Encarregada de Dados, implementará medidas que possibilitam entender os tratamentos de dados que estão acontecendo e, em caso de incidente de dados, adotar medidas concretas:
  - Gestão de permissões nos arquivos e pastas, por meio da implementação de controles de acesso de acordo com as classificações dos dados e informações;
  - Agendamento de treinamentos sobre a presente Política e sobre questões de proteção de dados e medidas de segurança;
  - Conscientização contínua de toda a equipe sobre a necessidade de manter as ferramentas, sistemas e aplicativos utilizados pelo Jubileu Sul Brasil atualizados, bem como do sistema de *firewall* da máquina e antivírus.



- Registrando as operações de tratamento de dados:

O mapeamento de dados pessoais do Jubileu Sul Brasil já foi realizado e trata-se de um documento orgânico e vivo, que deve ser adaptado e revisto para refletir a realidade atual da organização no que se refere às operações de tratamento de dados pessoais da organização. Este mapeamento é chamado de Registro das Operações de Tratamento (ROPA) e nele constam todas as atividades de tratamento de dados pessoais que nós realizamos no dia a dia da nossa organização. Este documento será periodicamente revisado pela Encarregada de Dados, com base nas atividades desenvolvidas pela organização que gerem novas operações de tratamento de dados pessoais.

Caso você, Colaborador, vá realizar uma atividade que envolva o tratamento de dados pessoais, será preciso preencher o **Formulário de Registro de Atividade de Tratamento de Dados Pessoais**, cujo modelo faz parte desta Política como seu **Anexo II**. A cada novo tratamento que for realizado, portanto, este registro será feito para:

- (a) Identificar a finalidade que justificará o tratamento de dados pessoais;
- (b) Identificar quais dados pessoais são necessários para atingir a finalidade, conforme exemplificado no Anexo I (“Glossário”), sempre levando em conta os princípios da LGPD, igualmente descritos no Anexo I;
- (c) Enquadrar o tratamento de dados a ser realizado em uma das bases legais previstas na LGPD, conforme Anexo I da Política;
- (d) Identificar se o Jubileu Sul Brasil atuará, no tratamento de dados pessoais em questão, como “Controlador” ou “Operador” e quem é o outro agente de tratamento e as responsabilidades de cada parte;
- (e) Identificar por quanto tempo o tratamento de dados pessoais em questão será necessário.

**O formulário, uma vez preenchido, deve ser encaminhado à Encarregada de Dados, para que faça a validação do conteúdo e avalie se as análises são pertinentes.** Com isso, a atividade será autorizada e a Encarregada de Dados poderá avaliar o nível de risco do tratamento de dados pessoais em questão, podendo adotar as medidas de segurança necessárias.

- Repassando as diretrizes contratuais à equipe do Jubileu Sul Brasil:

Quando iniciamos novas atividades com envolvimento de terceiros, existem contratos e/ou termos firmados para regular a atividade. Esses documentos trazem informações importantes relacionadas ao tratamento de dados. O Jubileu Sul Brasil e seus Colaboradores garantirão nos respectivos contratos e/ou termos que os agentes de tratamento, além de respeitar o Código de Ética e Conduta do Jubileu Sul Brasil:



- (a) Tratem dados pessoais somente mediante instruções documentadas do Jubileu Sul Brasil;
- (b) Implementem medidas técnicas e organizacionais apropriadas para garantir um nível de segurança adequado ao risco de tratamento;
- (c) Garantam que as pessoas autorizadas a tratar os dados pessoais tenham se comprometido com a confidencialidade ou estejam sob uma obrigação estatutária apropriada de confidencialidade;
- (d) Ajudem o Jubileu Sul Brasil a assegurar conformidade com as obrigações legais, incluindo, mas sem se limitar as seguintes: (i) implementação de medidas técnicas e organizacionais; (ii) notificação de violação ou incidente de segurança de Dados Pessoais; (iii) Conformidade com a LGPD;
- (e) Informem o Jubileu Sul Brasil sobre qualquer inspeção, auditoria ou inquérito realizado pela Autoridade Nacional de Proteção de Dados ou qualquer órgão regulador competente;
- (f) Notifiquem imediatamente o Jubileu Sul Brasil quando acreditarem razoavelmente que houve acesso, aquisição, perda, divulgação, destruição ou dano não autorizado ou acidental aos dados pessoais;
- (g) A critério do Jubileu Sul Brasil, eliminem ou devolvam todos os dados pessoais após o término da prestação de serviços relacionados ao tratamento, garantindo o retorno ou eliminação simultânea de cópias e dados pessoais arquivados;
- (h) Disponibilizem ao Jubileu Sul Brasil todas as informações necessárias para demonstrar a conformidade com as obrigações legais.
- (i) O Jubileu Sul Brasil garantirá que o agente de tratamento não subcontrate outro agente de tratamento sem autorização prévia por escrito específica ou geral do Jubileu Sul Brasil.

Recomendamos que o Jubileu Sul Brasil busque sempre formalizar suas relações utilizando contratos com cláusulas adaptadas à realidade do tratamento e gestão de dados aplicável. Cabe à Encarregada de Dados avaliar se determinada atividade pode ocorrer sem a formalização por meio de contrato e/ou termo.

## **V. COMO COMPARTILHAR DADOS PESSOAIS?**

O compartilhamento de dados pessoais acontece quando (i) dados coletados pelo Jubileu Sul Brasil forem compartilhados com terceiros ou (ii) quando o Jubileu Sul Brasil receber dados pessoais coletados por terceiros. Nestes casos, para garantir o cumprimento da LGPD, apresentamos as perguntas a seguir sobre as quais você, Colaborador, deve refletir quando estiver diante das situações (i) e (ii):



PERGUNTAS INICIAIS SOBRE O COMPARTILHAMENTO		
	Pergunta	Orientação
1	Os dados pessoais compartilhados são sensíveis?	A resposta à pergunta 1 indicará o <b>risco</b> envolvido no <b>compartilhamento de dados</b> , uma vez que os dados pessoais sensíveis podem colocar o Titular de Dados em situações de discriminação, se usados incorretamente
2	Os dados pessoais a serem compartilhados já são acessados pela parte que receberá os dados?	A resposta às perguntas 2 e 3 indica se pode existir o <b>risco de acesso indevido</b> ou <b>desvio de finalidade</b> por parte do terceiro para quem os dados pessoais estão sendo transferidos. Isso é importante para evitar que os dados sejam utilizados de forma diferente do que foi informado para os titulares de dados pessoais
3	Há risco/probabilidade da parte que recebeu os dados compartilhados utilizá-los para objetivos diferentes daqueles que foram informados aos Titulares de Dados Pessoais ou o compartilhamento ocorre justamente para que tal finalidade seja atingida?	

Após as reflexões pelas perguntas norteadoras acima, você deve seguir os passos:

	<i>[No caso de compartilhamento de dados pelo Jubileu Sul Brasil a terceiros]</i>	<i>[No caso de compartilhamento de dados com Jubileu Sul Brasil por terceiros]</i>
<b>Passo 1</b>	Seu gestor e a DPO precisam ser comunicados sobre a situação de compartilhamento. Para tanto, informar:	
1A	Com quem os dados pessoais serão compartilhados? <i>Ex: pessoa, consultar, empresa, outra OSC</i>	Quem está compartilhando os dados com o Jubileu Sul Brasil?
1B	Por qual motivo os dados pessoais serão compartilhados? <i>Ex: execução de parte de projeto comandado pelo Jubileu Sul Brasil; análise conjunta de uma mesma base de dados pessoais; prestação de contas sobre um projeto do Jubileu Sul Brasil, etc</i>	
1C	Quais as finalidades de utilização dos dados pessoais que serão compartilhados?	
1D	Existe relação contratual com este terceiro, com cláusula prevendo	Haverá ou houve formalização, por contrato, desta relação, prevendo a



	os cuidados que deverá ter com os dados pessoais transferidos pelo Jubileu Sul Brasil?	possibilidade de compartilhamento de dados pessoais?
<b>Passo 2</b>	Havendo a necessidade de compartilhamento de dados, a DPO analisará a operação de tratamento de dados pessoais que está sendo realizada e irá avaliar se este compartilhamento constitui uma nova finalidade que não foi informada anteriormente ao Titular, verificando os riscos do compartilhamento para o Jubileu Sul Brasil, e como coletar o consentimento do titular de dados para esta nova atividade, e se buscará fornecer a devida transparência sobre a atividade.	
<b>Passo 3</b>	A DPO irá analisar se o contrato ou termo firmado com o terceiro traz disposições detalhadas sobre proteção de dados e o tratamento de tais informações. Caso não haja contrato ou cláusulas sobre proteção de dados claras o suficiente, a DPO poderá recomendar que seja estabelecido um acordo de processamento de dados entre o Jubileu Sul Brasil e o terceiro.	
<b>Passo 4</b>	Após os passos anteriores, o compartilhamento de dados poderá ser realizado.	

## VI. O ARMAZENAMENTO E A RETENÇÃO DOS DADOS PESSOAIS

O Jubileu Sul Brasil reterá dados pessoais de forma consistente com suas obrigações legais e com suas políticas e procedimentos de retenção de dados. A LGPD disciplina o momento em que ocorre o término do tratamento dos dados e os motivos em que eles poderão continuar sendo armazenados pelo Controlador.

O Jubileu Sul Brasil deverá garantir que os dados pessoais sejam mantidos de forma a permitir a identificação do Titular de Dados Pessoais por um período não superior ao necessário para atingir a finalidade para qual os Dados Pessoais foram coletados e estejam sendo tratados.

A retenção consiste na continuidade de armazenamento dos dados pessoais pelo Jubileu Sul Brasil, caso haja motivo plausível, uma vez concluído seu tratamento e atingida a finalidade inicial para qual o dado pessoal foi coletado. Quando a finalidade do tratamento for atingida, se o prazo para o tratamento se encerrar ou se a autoridade de proteção de dados requisitar o encerramento, deve ser analisado se, de acordo com a LGPD, existe motivo plausível para continuar com o armazenamento das informações, analisando-se assim:

- (a) Se os dados são necessários para cumprimento de obrigação legal ou regulatória, ou seja, se existe algo nas leis e normas brasileiras que fundamente a manutenção do armazenamento;



- (b) Se o tratamento inicial estiver sendo realizado pelo Jubileu Sul Brasil para estudos ou pesquisas (utilizando esta base legal), garantindo sempre que possível a anonimização da base de dados;
- (c) Se a base de dados está anonimizada e sendo utilizada exclusivamente pelo Jubileu Sul Brasil.

**IMPORTANTE!** Quando a atividade de armazenamento posterior for considerada uma nova atividade de tratamento de dados, passaremos a reter os dados com base em algumas das hipóteses legais do art. 7º ou do art. 11 da LGPD. Essa decisão será tomada pela DPO.

Havendo motivos para o armazenamento de dados, será preciso registrar: **data de início do armazenamento, a finalidade deste armazenamento, prazo para armazenamento e data em que esse prazo se encerrará.** No **Anexo III** desta Política, você encontrará os prazos estabelecidos pelo Jubileu Sul Brasil para a retenção dos dados pessoais.

#### VII. COMO ELIMINAR DADOS PESSOAIS?

O Jubileu Sul Brasil eliminará dados pessoais com segurança quando:

- (i) Os dados pessoais não forem mais necessários para atingir as finalidades para as quais foram coletados;
- (ii) A autoridade de proteção de dados requisitar o encerramento do tratamento de dados pessoais;
- (iii) O Titular de Dados Pessoais revogar o consentimento para o tratamento dos dados pessoais;
- (iv) O Titular de Dados Pessoais se opuser ao Tratamento e não houver outro fundamento legal para o tratamento; ou
- (v) Os dados pessoais tiverem sido tratados em desconformidade com a LGPD.

A operação de eliminação, exclusão ou descarte também é considerada como atividade de tratamento pela LGPD, e, por esta razão, existem cuidados que devem ser adotados no procedimento:

- Documentos físicos:
  - Para documentos com dados de alto risco, em que constam dados considerados sensíveis, confidenciais, sigilosos ou pelo seu teor trazer riscos para o Jubileu Sul Brasil, recomenda-se a utilização de caneta/carimbo selador de dados confidenciais. Ele é ideal para



esconder/omitir informações dificultando ou tornando impossível a identificação dos dados.

- Utilização de fragmentadoras de papel, devendo-se priorizar os equipamentos que permitem deixar o papel mais triturado pois quanto menores os pedaços, mais difícil a recuperação e associação das informações neles constantes.
- **Documentos digitais:**
  - Averiguar contratualmente ou nos termos de uso e política de privacidade do sistema de armazenamento por qual período, após a eliminação do dado no sistema, eles mantêm a informação no backup.
  - Quando o Jubileu Sul estiver na posição de Controlador: deve encaminhar comunicado a todos os operadores de dados que tratem os dados objeto da eliminação para repetirem o procedimento utilizado e descartem os dados de forma correta, segura e no prazo determinado pelo Jubileu Sul Brasil.
  - Quando o Jubileu Sul Brasil estiver na posição de Operador: deve se atentar às determinações do Controlador sobre o procedimento que deve ser utilizado para o descarte dos dados.

#### VIII. A ENCARREGADA DE DADOS

A **Encarregada de Dados** é também chamado de **DPO** (*Data Protection Officer*). Trata-se de cargo previsto na LGPD, tendo por função ser o ponto de contato entre os titulares de dados pessoais, a Autoridade Nacional de Proteção de Dados (ANPD) e o Jubileu Sul Brasil.

A Encarregada de Dados, assim como sua substituta, no caso de sua ausência, impedimento ou vacância, tem as seguintes competências:










- (a) Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- (b) Receber comunicações da ANPD e adotar providências;
- (c) Orientar os Colaboradores do Jubileu Sul Brasil a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- (d) Executar as demais atribuições determinadas pelo Jubileu Sul Brasil ou estabelecidas em normas complementares;
- (e) Avaliar os formulários de registro de atividade de tratamento de dados pessoais e prestar esclarecimentos aos Colaboradores sempre que necessário;
- (f) Liderar o Comitê de Gestão de Crise, no caso de incidente de segurança de dados pessoais, assim como a organização e implementação de planos de respostas e remediação a tais incidentes;



- (g) Coordenar a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD);
- (h) Estruturar os processos para manutenção do Registro das Operações de Tratamento (ROPA) e revisá-lo periodicamente, pelo menos a cada 6 meses;
- (i) Levar ao conhecimento de todos da organização todas as conclusões e instruções sobre os riscos envolvidos em casos identificados de inadequação à LGPD;
- (j) Promover treinamentos periódicos acerca da presente Política; e
- (k) Avaliar situações de compartilhamento de dados pessoais com ou de terceiros, identificando a necessidade de contratos e termos para tanto e monitorar sua contínua execução.

### 1. Comunicação de titulares e procedimentos de resposta

Os titulares de dados pessoais poderão exercer os seguintes direitos, previstos na LGPD, perante o Jubileu Sul Brasil, os quais serão recebidos, registrados e respondidos pela Encarregada de Dados:

- |  |  |
|--|--|
|  Confirmação do tratamento dos pessoais e obter informações sobre este processamento.                             |  Acesso aos dados pessoais tratados pelo Jubileu Sul Brasil.  |
|  Correção de dados incompletos, inexatos ou desatualizados.   |  Solicitar anonimização, bloqueio ou a eliminação de dados desnecessários, excessivos ou já tratados pelo Jubileu Sul Brasil. |
|  Direito de solicitar a transmissão dos dados tratados pelo Jubileu Sul Brasil para outro fornecedor de serviços. |  Eliminação dos dados pessoais tratados com base no consentimento.  |
|  Obter informações sobre compartilhamento de dados pessoais.  |  Revogar o consentimento e obter informações sobre esta possibilidade e sobre a consequência de não fornecer o consentimento. |
|  Revisão de decisões automatizadas que afetem seus interesses.  |  |

Ao receber o pedido, a Encarregada de Dados buscará compreensão sobre (i) confirmar a identidade do titular de dados; (ii) qual projeto ou atividade os dados atrelados à requisição diz respeito; (iii) avaliar se existem parceiros ou terceiros em seu nome realizando tratamento de dados pessoais do titular em questão, para verificar se é o caso de notificá-lo; e (iv) identificar qual o direito que está sendo exercido pelo titular e avaliar a possibilidade de atendimento integral, parcial ou a impossibilidade de executar o pedido.





Após o atendimento integral, parcial ou a conclusão pela impossibilidade de executar o pedido do titular de dados, a DPO deverá responder o titular com as informações adequadas à situação. No caso de pedido de eliminação ou anonimização do banco de dados, deve-se verificar qual a base legal que sustenta o tratamento (se for o consentimento, deve-se promover a retirada do mesmo; se for outra base legal, deve-se avaliar se a finalidade do tratamento do dado já se encerrou e se é possível atender ao pedido neste momento).

**IMPORTANTE!** Deve ser mantido o registro das solicitações de titulares de dados bem como do conteúdo das respostas encaminhadas pela DPO para cumprimento do princípio da LGPD de responsabilização e prestação de contas.

## 2. Comunicação da ANPD e procedimento de resposta

Eventualmente, a ANPD poderá entrar em contato com o Jubileu Sul Brasil para obter maiores informações sobre as atividades de tratamento de dados pessoais que desempenha.

No caso do recebimento de demanda da ANPD, o Jubileu Sul Brasil, por meio de sua Encarregada de Dados, registrará o pedido da ANPD e buscará compreensão sobre: (i) em qual atividade ou projeto os dados pessoais atrelados à requisição da ANPD são ou foram tratados; (ii) se existem parceiros ou terceiros em nome do Jubileu Sul Brasil realizando tratamento dos dados do titular de dados em questão, para verificar se é o caso de notificá-lo; e (iii) qual o direito está sendo pontuado pela ANPD. No caso de parceiros ou terceiros envolvidos no tratamento do dado pessoal em questão, a DPO notificará para que repliquem sua atuação na resolução da requisição.

**IMPORTANTE!** Deve ser mantido o registro das solicitações da ANPD bem como do conteúdo das respostas encaminhadas pela DPO para cumprimento do princípio da LGPD de responsabilização e prestação de contas. Além disso, a DPO deverá monitorar o processo e acompanhar se o problema ou solicitação da ANPD foi atendida em sua integralidade.

## IX. VIOLAÇÃO DE DADOS E INCIDENTES DE SEGURANÇA

Se a qualquer momento, você, Colaborador, tomar conhecimento de qualquer violação de dados ou incidente de segurança que possa levar ou tenha levado à destruição, perda, alteração, divulgação ou acesso não autorizado de dados pessoais, ou ainda, acreditar que dados pessoais são ou foram tratados em violação a esta Política, você deve comunicar imediatamente a Encarregada de Dados, com as seguintes informações:



- Nome do Projeto, atividade ou área afetada;
- Qual a ocorrência, data e hora do incidente;
- Quais dados foram vazados e onde ocorreu o vazamento (se já tiver sido identificado);
- Quais medidas já foram adotadas (se for o caso);
- Apontar se já houve comunicação com o titular de dados pessoais;
- Demais informações a respeito do incidente ou qualquer outra que possa ter sido utilizada para identificá-lo.

Como **diretrizes internas na eventualidade de Incidente de segurança da informação**, deve-se seguir os seguintes passos:

1. **Notificação interna sobre incidente com dados pessoais:** caso a Encarregada de Dados identifique ou seja notificado internamente da ocorrência de um incidente de segurança, será instituído um **Comitê de Gestão de Crise** para atuação imediata.

#### **Comitê de Gestão de Crise**

##### Composição:

Encarregada de Dados: **Rosilene Wansetto**

Substituta da Encarregada de Dados: **Lucimeire Araujo de Souza Paludette**

Presidente da Diretoria: **Talita de Oliveira Guimarães**

Outros membros do Comitê de Gestão de Crise: **Joilson José Costa, Diretor Secretário; Karina da Silva Pereira, Diretora Financeira, Alessandro Lima, TI; Flaviana Serafim, Assistente de Comunicação.**

Convidados externos (consultivos): SBSA Advogados e outras consultorias que se façam necessárias.

2. **Avaliação de risco do incidente com dados pessoais:**

Quando ciente da ocorrência de um incidente com dados pessoais, o Jubileu Sul Brasil deverá providenciar, através do Comitê de Gestão de Crise e da Encarregada de Dados, a avaliação do risco atrelado à situação. Como se trata de uma atuação técnica jurídica, acionaremos o escritório SBSA Advogados, como ponto de apoio para a definição de riscos regulatórios e de direitos humanos envolvidos.

A mensuração do risco é essencial para identificar a necessidade de publicização do incidente por meio de notificação à ANPD ou aos titulares de dados pessoais. Isso porque somente o risco de dano relevante para os titulares de dados deve ser notificado,



ou seja, situações nas quais os titulares dos dados podem ter sido colocados em risco. Esta mensuração considerará tanto o volume de dados pessoais acessados a partir do incidente quanto à sensibilidade de dados pessoais afetados.

É importante ter em mente que nem todo incidente precisa ser comunicado à ANPD ou, muito menos, aos titulares de dados pessoais. Deve-se considerar que, dependendo da área, projeto ou atividade do envolvido, o nível de risco decorrente do incidente de dados pessoais pode ser diferente, uma vez que, existem diversos tipos de dados pessoais sendo tratados no Jubileu Sul Brasil, para finalidades diversas.

**3. Adoção dos procedimentos externos:** além dos procedimentos internos indicados anteriormente, poderá ser necessário comunicar agentes externos como Autoridades (Ex: ANPD), os titulares de dados pessoais afetados e/ou parceiros. É obrigação do Jubileu Sul Brasil, quando Controlador, comunicar à ANPD e ao titular de dados pessoais no caso de risco ou dano relevante para os titulares, ainda que haja dúvida sobre a relevância dos riscos e danos envolvidos.

**a. Comunicação à ANPD e outras autoridades sobre o incidente com dados pessoais:**

- Sempre que o Incidente de segurança puder acarretar um risco ou dano relevante aos titulares afetados, deverá ser comunicado à Autoridade Nacional de Proteção de Dados (ANPD). A comunicação poderá ser parcial (preliminar), nas hipóteses em que as informações sobre o Incidente ainda estão sendo apuradas, por exemplo.
- Segundo recomendações da própria ANPD, o **prazo para a comunicação é de 2 (dois) dias úteis**, contado da ciência do Incidente. A comunicação à ANPD deve ser feita por meio do formulário disponibilizado pelo órgão em seu [site](#).
- A depender do incidente de segurança, como, por exemplo, na hipótese de ocorrência de um crime cibernético (aqueles que ocorrem no meio digital), será necessário acionar também autoridades policiais.
- Para esta comunicação, as informações devem ser claras e concisas, contendo ao menos, de acordo com a LGPD e orientações da ANPD:
  - (i) A descrição da natureza dos dados pessoais afetados; as informações sobre os titulares envolvidos;
  - (ii) A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
  - (iii) Os riscos relacionados ao incidente;
  - (iv) Os motivos da demora, no caso de a comunicação não ter sido imediata;



- (v) As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo;
  - (vi) Identificação dos responsáveis pelo tratamento e da Encarregada de Dados Pessoais;
  - (vii) Demais informações relevantes sobre o incidente de segurança com dados pessoais.
- Quanto mais informações forem fornecidas à ANPD, mais fácil será identificar os responsáveis e prevenir a ocorrência de danos aos titulares, pelos quais o Jubileu Sul Brasil poderá ser responsabilizado.

**b. Comunicação dos titulares sobre o incidente com dados pessoais:**

- O Jubileu Sul Brasil informará aos titulares de dados pessoais afetados, sem demora justificada, sobre qualquer violação da segurança de seus dados pessoais, quando legalmente assim exigido e fornecerá todas as informações necessárias exigidas pela LGPD.
- Sempre que ocorrer um incidente de segurança de dados pessoais, acidental ou ilícito, que possa acarretar um risco ou dano relevante aos titulares afetados, o Jubileu Sul Brasil irá informá-los de maneira clara e concisa, indicando um resumo das medidas implementadas até o momento para controlar os possíveis danos.
- Algumas das hipóteses em que estará obrigado o Jubileu Sul Brasil a fazer tal comunicação são quando:
  - Envolver dados sensíveis ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes;
  - Tiver o potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade;
  - Envolver um grande volume de dados;
  - Afetar muitos indivíduos;
  - Envolver má-fé de terceiros que tiveram acesso aos dados após o incidente;
  - Possibilitar com facilidade a identificação dos titulares por terceiros não autorizados.
- Havendo dúvida sobre a relevância dos riscos e danos envolvidos, a comunicação deve ser efetuada.

**4. Diretrizes específicas para a comunicação institucional e assessoria de imprensa:**

- a. Manter a coerência e estabilidade do discurso, sempre alinhado previamente com o Comitê de Gestão de Crise e contemplando a máxima preocupação com o titular de dados afetado.



- b. Caso a equipe de resposta determine a comunicação sobre o Incidente aos titulares dos Dados Pessoais afetados, a Encarregada de Dados irá desenvolver a mensagem da comunicação, priorizando: (i) dar transparência dos fatos ocorridos; (ii) apontar as medidas já tomadas pelo Jubileu Sul Brasil para minimizar o impacto dos efeitos; (iii) eventuais medidas ao alcance dos próprios titulares para mitigar riscos de efeitos adversos; e (iv) indicar os canais de contato para sanar dúvidas.
- c. Nunca deixar uma demanda/pergunta de jornalista, autoridade pública ou sociedade sem resposta.

#### **X. VIOLAÇÃO À POLÍTICA**

O Jubileu Sul Brasil garantirá o cumprimento desta Política pelos seus Colaboradores. A não conformidade com esta Política é considerada violação do Código de Ética e Conduta do Jubileu Sul Brasil e poderá resultar em sanções disciplinares, demissão ou qualquer outro tipo de sanção permitida pela lei brasileira.

O não cumprimento dessa Política, por algum Colaborador, poderá, ainda, acarretar sanções administrativas em primeira instância (bloqueio de acessos e recolhimento de equipamentos), podendo ainda levar ao desligamento do empregado, dependendo da gravidade da ocorrência. A decisão sobre aplicabilidade de sanção ou penalidade está sob responsabilidade da Diretoria do Jubileu Sul Brasil, ou ainda do Assembleia Geral nos casos em que a Diretoria possa ser parte interessada.



## ANEXO I – Glossário

### Definições

#### Anonimização

Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, que faz com que o dado perca a possibilidade de associação, direta ou indireta, com o seu titular. Para ser anonimização, o processo não pode ser revertido, o anonimato necessita ser definitivo.

#### Controlador

Qualquer pessoa natural ou jurídica que atuar tomando as decisões sobre o tratamento dos dados.

#### Dado pessoal

São as informações relativas à pessoa, que permitem sua identificação, ou, como consta da LGPD “informação relacionada à pessoa natural identificada ou identificável”, o que pode incluir, além de nome, e-mail, CPF, entre outros identificadores que, se analisados em conjunto, permitem a identificação do titular de dados.

#### Dado pessoal sensível

São dados sobre origem racial, étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou a vida sexual, dado genético ou biométrico.

#### Descarte

É o ato de excluir, deletar e/ou eliminar os dados pessoais, pode ser virtual ou fisicamente.

#### Encarregado(a) de Dados (DPO)

É o responsável por monitorar e garantir o funcionamento da estrutura de governança de dados, criada para adequar a organização/empresa à LGPD sendo o ponto de contato entre os titulares, a Autoridade Nacional de Proteção de Dados e o Jubileu Sul Brasil.

#### LGPD

Lei Geral de Proteção de Dados - Lei nº 13.709/2018

#### Retenção

É o ato de armazenar os dados pessoais após o período de tratamento ativo para cumprimento

da finalidade para o qual o dado foi coletado, pode ser virtual ou fisicamente.

#### Titular de dados

É a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

#### Tratamento de dados

Toda operação e/ou ação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

### Princípios

#### (Artigo 6º, LGPD)

#### Boa-fé

Significa a observância de um comportamento leal, correto e probó na realização das atividades de tratamento de dados pessoais. Esse princípio, opera como norte a todos os demais e serve de baliza para interpretar conceitos abertos (art. 6º, caput, LGPD).

#### Finalidade

É a realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

#### Adequação

É a compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

#### Necessidade

É a limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

#### Livre acesso

É a garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do



tratamento, bem como sobre a integralidade de seus dados pessoais.

### Qualidade dos dados

É a garantia aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

### Transparência

É a garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

### Segurança

É a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

### Prevenção

Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

### Não discriminação

É a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

### Responsabilização e prestação de contas

Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

### Bases legais

*(Artigo 7º, LGPD - dados pessoais)*

#### Consentimento

Declaração do titular de que concorda com o uso de seus dados pessoais para uma determinada finalidade. Devendo ser sempre livre, inequívoco e informado.

#### Obrigação legal

O tratamento de dados é justificado pela obrigação de cumprir outras leis.

### Políticas Públicas

Utilizada pela Administração Pública para a execução de políticas públicas previstas em leis, contratos, convênios ou similares.

### Execução de contrato

Quando necessário para (i) a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; ou (ii) a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais

### Exercício regular de direitos

Permite que o tratamento dos dados pessoais seja assegurado para exercício de direitos em processo judicial, administrativo ou arbitral

### Proteção da vida

Utilizada para a proteção da vida ou da incolumidade física do titular ou de terceiro.

### Tutela da saúde

Para tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

### Legítimo interesse

Pode ser utilizado como base legal para o tratamento de dados pessoais sem o consentimento, desde que essas ações não violem os direitos e liberdades fundamentais do titular e tenham fins de tratamento justificáveis

### Proteção ao crédito

Para avaliar o histórico da pessoa, visando assim a aprovação de crédito e a redução de riscos na transação.

### Bases legais

*(Artigo 11, LGPD - dados sensíveis)*

#### Consentimento

Declaração do titular de que concorda com o uso de seus dados pessoais para uma finalidade específica e em destaque. Devendo ser sempre livre, inequívoco e informado.

#### Obrigação legal

O tratamento de dados é justificado pela obrigação de cumprir outras leis.



### Políticas

#### Públicas

A Administração Pública poderá se valer de dados sensíveis, nas situações em que tal for indispensável para execução de políticas públicas previstas em leis ou regulamentos.

#### Exercício regular de direitos

Permite que o tratamento dos dados pessoais seja assegurado para exercício de direitos em contrato, processo judicial, administrativo ou arbitral

#### Proteção da vida

Utilizada para a proteção da vida ou da incolumidade física do titular ou de terceiro.

#### Tutela da saúde

Para tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

#### Garantia de prevenção à fraude e à segurança do titular

Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Dados pessoais Art. 7º da LGPD	Dados sensíveis Art. 11 da LGPD
Consentimento	✓
Obrigação legal	✓
Políticas públicas	✓
Órgão de pesquisa	✓
Execução de contratos	✗
Exercício regular de direitos	✓
Proteção da vida	✓
Tutela da saúde	✓
Legítimo interesse	✗
Proteção de crédito	✗
	Garantia de prevenção à fraude e à segurança do titular

Figura 1. A imagem acima esclarece quais bases legais podem ser utilizadas para dados pessoais (art. 7º, LGPD) e para dados pessoais sensíveis (art. 11, LGPD).





## ANEXO II – Modelo de Formulário de Registro de Atividade de Tratamento de Dados Pessoais

Os Colaboradores que realizarem operações de tratamento de dados pessoais em nome do Jubileu Sul Brasil devem preencher o formulário abaixo para devido registro da atividade, a cada novo tratamento realizado pelo Jubileu Sul Brasil.

Por “dado pessoal”, conforme Anexo I (“Glossário”) da Política Interna de Privacidade e Proteção de Dados do Jubileu Sul Brasil, entende-se: “a informação relacionada à pessoa natural identificada ou identificável, incluindo, sem limitação, números identificativos, dados locacionais, identificadores eletrônicos, dados que possam ser combinados com outras informações para identificar um indivíduo, e/ou que se relacionem com a identidade, características ou comportamento de um indivíduo ou influenciem na maneira como esse indivíduo é tratado ou avaliado”.

Formulário de Registro de Atividade de Tratamento de Dados Pessoais	
Projeto ou Atividade relacionado	
Colaborador(es) Responsável(is)	
Por que vamos usar os dados pessoais?	<i>Indicar a finalidade que justificará o tratamento de dados pessoais.</i>
Quais dados pessoais serão coletados?	<i>Indicar quais dados pessoais são necessários para atingir a finalidade, conforme tabela exemplificativa no Anexo I (“Glossário”) da Política Interna de Privacidade e Proteção de Dados Pessoais. Não há necessidade de indicar os dados pessoais em si, mas quais tipos de dados (endereço, nome, CPF, e-mail, por exemplo).</i>
Como o Jubileu Sul Brasil irá operacionalizar o uso desses dados pessoais? Será compartilhado com terceiros?	<i>Identificar se o Jubileu Sul Brasil atuará no tratamento de dados pessoais em questão como “Controlador” ou como “Operador” e quem é(são) o(s) outro(s) agente(s) de tratamento envolvidos. Caso haja dúvida sobre tais conceitos, recomendamos a consulta ao Anexo I (“Glossário”) da Política Interna de Privacidade e Proteção de Dados. Haverá terceiros envolvidos em alguma etapa do tratamento de dados pessoais?</i>
Por quanto tempo vamos precisar destes dados pessoais?	<i>Identificar por quanto tempo o tratamento de dados pessoais em questão se mostra necessário para os objetivos da atividade ou projeto, além da expectativa de armazenamento/retenção desses dados.</i>



## ANEXO III – Prazos de Retenção

IV.1. Documentos trabalhistas e previdenciários		Explicação	
		De forma geral, a recomendação de prazos de retenção para documentos trabalhistas é de 5 (cinco) anos após o término da relação de trabalho com o colaborador. Isto porque a Constituição Federal, em seu art. 7, XXIX, garante ao trabalhador este mesmo prazo prescricional para a pretensão da ação trabalhista. Devido à possibilidade de reclamação trabalhista, portanto, admite-se que o empregador retenha todo tipo de dado que possa servir-lhe como prova e defesa no curso do processo judicial.	
Lista de Prazos			
Documento	Prazo de retenção	Início da contagem	Fundamento legal
Acordo de compensação de horas	5 anos	Término da relação laboral	CF, artigo 7º, inciso XXIX
Acordo de prorrogação de horas	5 anos	Término da relação laboral	CF, artigo 7º, inciso XXIX
Autorização de descontos	5 anos	Término da relação laboral	CF, artigo 7º, inciso XXIX
Aviso Prévio e pedido de demissão	5 anos	Término da relação laboral	CF, artigo 7º, inciso XXIX
Carta de pedido de demissão	5 anos	Término da relação laboral	CF, artigo 7º, inciso XXIX
CAT - Comunicação de Acidente de Trabalho	5 anos	Término da relação laboral	CF, artigo 7º, inciso XXIX
Comprovante de entrega da GPS (Guia da Previdência Social) ao sindicato profissional	5 anos	Primeiro dia do exercício anual seguinte	Art. 578/579 CLT e art. 173/217 CTN
Comprovante de pagamento ou a declaração apresentada pelo contribuinte individual para fins de apresentação ao INSS	5 anos	Data do recolhimento	CF, artigo 7º, inciso XXIX
Ficha de Acidente de Trabalho, Formulário Resumo Estatístico Anual/Mapa de avaliação dos acidentes de Trabalho (SESMT)	5 anos	Primeiro dia do exercício seguinte	Portaria 3.214/78 - Norma Regulamentadora nº 4, item 4.12.1
GPS (Guia da Previdência Social) original	5 anos	Primeiro dia do exercício seguinte	Art. 45, Lei 8.212/91 c/c Súmula vinculante nº 8 STF
GRCS (Guia de Recolhimento da Contribuição Sindical)	5 anos	Primeiro dia do exercício seguinte	Arts. 578/579, CLT c/c arts. 173 e 217 CTN
Livros, cartão ou fichas de ponto	5 anos	Término da relação laboral	CF, artigo 7º, inciso XXIX
RAIS (Relação Anual de Informações Sociais)	5 anos	Primeiro dia do exercício seguinte	Art. 9º, Portaria MTE 651/07
Recibo de entrega de vale transporte	5 anos	Término da relação laboral	CF, artigo 7º, inciso XXIX
Recibo de pagamento de salários	5 anos	Término da relação laboral	CF, artigo 7º, inciso XXIX



Recibo de pagamento de férias	5 anos	Término da relação laboral	CF, artigo 7º, inciso XXIX
Recibo de pagamento de 13º salários	5 anos	Término da relação laboral	CF, artigo 7º, inciso XXIX
Salário-educação - documentos relacionados ao benefício	5 anos	Término da relação laboral	CF, artigo 7º, inciso XXIX
Salário-família - documentos relacionados ao benefício	5 anos	Término da relação laboral	CF, artigo 7º, inciso XXIX
Salário-maternidade - documentos relacionados ao benefício	5 anos	Término da relação laboral	CF, artigo 7º, inciso XXIX
Seguro-desemprego (Comunicação de Dispensa - CD e Requerimento do Seguro-Desemprego - SD)	5 anos	Término da relação laboral	CF, artigo 7º, inciso XXIX
TRCT - Termo de Rescisão do Contrato de Trabalho	5 anos	Término da relação laboral	CF, artigo 7º, inciso XXIX
Comprovante de pagamento de benefícios reembolsados pelo INSS	5 anos	Primeiro dia do exercício seguinte	Dec. 3.048/99, art. 348
DARF - PIS (Programa de Integração Social)	10 anos	Data do recolhimento	Dec.-Lei nº 2.052/83 - art. 3º
Folha de pagamento	10 anos	Primeiro dia do exercício seguinte	Dec. 3.048/99, art. 225,01, § 5º
Atestado de saúde ocupacional	20 anos	Término da relação laboral	Portaria SSST nº 24/94, item 7.4.5.1
Histórico clínico	20 anos	Término da relação laboral	Portaria SSST nº 24/94, item 7.4.5.1
PPP - Perfil Profissional Profissiográfico	20 anos	Término da relação laboral	Art. 266, § 9º - Instrução Normativa INSS Nº 77/2015
Registro do PPRA (Programa de Prevenção de Riscos Ambientais)	20 anos	Término da relação laboral	Portaria SSST nº 25/94, item 9.3.8.2
Registro do PCMSO (Programa de Controle Médico de Saúde Ocupacional).	20 anos	Término da relação laboral	Norma Regulamentadora nº 7
Depósito de FGTS (GFIP - Guia de Recolhimento do Fundo de Garantia do Tempo de Serviço e Informações à Previdência Social)	30 anos (a partir de 13/11/2019 o prazo diminui para 5 anos)	Data do recolhimento	Art. 23-A, § 3º, Lei nº 8.036/90
Guia de Recolhimento Rescisório do FGTS (GRRF)	30 anos (a partir de 13/11/2019 o prazo diminui para 5 anos)	Data do recolhimento	Art. 23-A, § 3º, Lei nº 8.036/90
RE - Relação de Empregados do FGTS	30 anos (a partir de 13/11/2019 o prazo	Primeiro dia do exercício seguinte	Art. 23-A, § 3º, Lei nº 8.036/90



	diminui para 5 anos)		
CAGED - Cadastro Geral de Empregados e Desempregados	3 anos	Primeiro dia do exercício seguinte	Portaria nº 2.115/99, art. 1º § 2º
CIPA - Comissão Interna de Prevenção de Acidentes - livros de atas	5 anos	Data de início do próximo processo eleitoral	Portaria 3.214/78 - Norma Regulamentadora nº 5, item 5.9.2
Contrato de trabalho	30 anos (prazo mais longo determinado na tabela)	N/A	N/A
Livro de Inspeção do Trabalho	30 anos (prazo mais longo determinado na tabela)		
Livros ou fichas de registro de empregados	30 anos (prazo mais longo determinado na tabela)	N/A	N/A

		Explicação	
<p><b>IV.2. Documentos relacionados a processos de contratação</b></p>		<p>Alguns documentos obtidos em função da prospecção e processo seletivo de novos colaboradores do GIFE também poderão ser mantidos, contanto que o titular seja notificado sobre a retenção. No entanto, no caso de o candidato não ter sido selecionado não existe a possibilidade de tratamento com base legal na execução de contrato, a retenção destes documentos poderá ser considerada como hipótese de legítimo interesse do GIFE, sujeita a um regramento mais rigoroso por parte da LGPD. Sendo assim, recomendamos que os documentos abaixo sejam retidos por tão curto tempo quanto possível, especialmente no caso de candidatos rejeitados.</p>	
		Lista de Prazos	
Documento	Prazo de retenção	Início da contagem	Fundamento legal
Formulários de inscrição em processos seletivos	Máximo de 1 (um) ano	Entrega do formulário pelo candidato	Lei Geral Brasileira de Proteção de Dados (Lei nº 13.709/2018, ou LGPD), art. 15, I, II e III e art. 16
<p><i>Obs: Não há nenhuma determinação na legislação trabalhista que possa fornecer parâmetros para o descarte de informações de candidatos a vagas de emprego. No entanto, toda informação pessoal deve ser descartada uma vez concluída a finalidade para qual foi coletada ou outra finalidade legítima informada aos titulares. Caso a organização inclua uma notificação a respeito da atividade de retenção dos dados para finalidade de contato posterior, terá legitimidade para a retenção. Acreditamos que um prazo de 1 (um) ano é razoável para tal atividade, dado que o contato posterior após este período costuma ser raro entre as organizações.</i></p>			
Notas de entrevistas e resultados de exercícios	Máximo de 1 (um) ano	Elaboração das anotações e notas	Lei Geral Brasileira de Proteção de Dados (Lei nº 13.709/2018, ou LGPD), art. 15, I, II e III e art. 16
Background check de qualificações e referências	Máximo de 1 (um) ano	Elaboração dos registros	Lei Geral Brasileira de Proteção de Dados (Lei nº 13.709/2018, ou



			LGPD), art. 15, I, II e III e art. 16
Background check de registros criminais	Máximo de 6 (seis) meses	Elaboração dos registros	Lei Geral Brasileira de Proteção de Dados (Lei nº 13.709/2018, ou LGPD), art. 15, I, II e III e art. 16

IV.3. Documentos financeiros		Explicação	
		<p>Muitos dos documentos financeiros contêm dados pessoais, ainda que em caráter acessório. A necessidade de retenção de alguns documentos para fins de obrigação legal e regulatória permite que sejam retidos pelo controlador sob a hipótese do art. 16, I, da LGPD, ou seja, sem necessidade de notificação do titular dos dados sobre a finalidade específica do armazenamento. A retenção devido à possibilidade de ajuizamento de demandas relacionadas aos processos financeiros, apesar de conferir legitimidade para o armazenamento por maiores períodos, não configura obrigação legal e deve, também, ser informada aos titulares.</p> <p>Quando há conflito de prazos (por exemplo, recomendações de retenção por ordem trabalhista e fiscal, o controlador terá direito ao armazenamento dos dados pelo prazo maior).</p>	
Lista de Prazos			
Documento	Prazo de retenção	Início da contagem	Fundamento legal
Reembolso de funcionários	Para fins fiscais: 5 (cinco) anos	Para fins fiscais: A partir do primeiro dia do exercício seguinte àquele em que o lançamento poderia ter sido efetuado.	Código Tributário Brasileiro (CTN), art. 150, art. 173 e art. 174 Código Tributário Brasileiro (CTN), art. 195, parágrafo único
	Para fins trabalhistas: 6 (seis) anos	Para fins trabalhistas: desde o término da relação com o trabalhador	CF, artigo 7º, inciso XXIX
<i>Obs: Qualquer um dos prazos que seja maior. Este prazo poderá ser estendido, caso ocorra alguma fiscalização.</i>			
Comprovação do registro de pagamento de seguro de vida e impostos	Para fins fiscais: 5 (cinco) anos	Para fins fiscais: A partir do primeiro dia do exercício seguinte àquele em que o lançamento poderia ter sido efetuado	Código Tributário Brasileiro (CTN), art. 150, art. 173 e art. 174 Código Tributário Brasileiro (CTN), art. 195, parágrafo único
	Para fins trabalhistas: 6 (seis) anos	Para fins trabalhistas: desde o término da relação com o trabalhador	CF, artigo 7º, inciso XXIX
<i>Obs: Qualquer um dos prazos que seja maior. Este prazo poderá ser estendido, caso ocorra alguma fiscalização.</i>			



IV.4. Documentos de segurança		Explicação	
		Documentos necessários à segurança física dos espaços da organização ou da idoneidade de seus espaços virtuais.	
Lista de Prazos			
Documento	Prazo de retenção	Início da contagem	Fundamento legal
Controle de entrada e saída do estabelecimento físico da organização (ex.: CCTV)	1 (um) ano.	Data da coleta dos dados	Lei Geral Brasileira de Proteção de Dados (Lei nº 13.709/2018, ou LGPD), art. 15, I, II e III e art. 16
<i>Obs: Não há prazo legalmente definido para a retenção dos dados de segurança e proteção. Porém, o descarte deve ser feito, no mínimo, a cada 1 ano contado da coleta dos dados ou, se possível, a cada seis meses.</i>			
Registros de conexão nos sistemas detidos pela organização (ex: plataforma web )	6 meses	Data da coleta dos dados	Marco Civil da Internet (Lei nº 12.965/14)

IV.5. Contratos e Comunicações com pessoas participantes em projetos e eventos		Explicação	
		Documentos-padrão para realização de eventos e projetos, contendo, principalmente dados de pessoas participantes.	
Lista de Prazos			
Documento	Prazo de retenção	Início da contagem	Fundamento legal
Contratos com pessoas participantes nos projetos	11 (onze) anos	Última prestação (em caso de contratos verbais) ou data de encerramento do contrato	Código Civil Brasileiro (Lei nº 10.406/2002), art. 205 e Recurso Especial 1.280.825/SP
<i>Obs: O STJ pacificou que o prazo prescricional para ação em matéria contratual é de 10 (dez) anos. A mera prestação de serviços pode contar como contrato verbal, de forma que qualquer coleta de dados feita para seu cumprimento se inclui na presente hipótese.</i>			
Formulários, listas de presença, entrevistas e documentos gerais de registro dos projetos (apenas dados comuns)	Indeterminado	Conclusão do projeto	Lei Geral Brasileira de Proteção de Dados (Lei nº 13.709/2018, ou LGPD), art. 15, I, II e III e art. 16
<i>Obs: A organização poderá armazenar os dados para fins de reter a memória dos projetos concluídos. Este armazenamento, no entanto, será feito em interesse legítimo da organização, representando uma nova atividade de tratamento em relação à realização do projeto em si. Recomendamos, nestes casos, o envio de uma notificação aos titulares de dados a respeito da retenção de seus dados com possibilidade de opt-out, ou seja, solicitação de exclusão ou anonimização dos próprios dados da base armazenada</i>			
Formulários, listas de presença, entrevistas e documentos gerais de registro dos projetos (se houver dados sensíveis)	Imediatamente	Após a consecução da finalidade do projeto	Lei Geral Brasileira de Proteção de Dados (Lei nº 13.709/2018, ou LGPD), art. 15, I, II e III e art. 16
<i>Obs: Quanto aos dados sensíveis coletados (ou dados especialmente expositivos, como antecedentes criminais), caso possível, recomendamos a pronta anonimização diante da conclusão do projeto. É dizer, podem-se manter os dados de forma desvinculada dos indivíduos a quem se referem - por exemplo, na forma de relatórios estatísticos e apresentações de dados agregados. Porém, os documentos que estabelecem conexões entre estes dados e um indivíduo devem ser alterados.</i>			



Prospecção de novos projetos	Imediatamente	Após a consecução da finalidade	Lei Geral Brasileira de Proteção de Dados (Lei nº 13.709/2018, ou LGPD), art. 15, I, II e III e art. 16
<i>Obs: A retenção de dados pessoais decorrente da prospecção de novos projetos teria, como base legal, apenas o interesse legítimo da organização. Sendo assim, os titulares deverão ser notificados a respeito de tal e recomendamos o descarte mais célere possível de todos os dados desnecessários a uma finalidade específica.</i>			
Documentos com potencial de subsídio em processo de indenização por danos às pessoas participantes nos projetos	3 (três) anos	Desde o incidente originador do dano	Código Civil Brasileiro (Lei nº 10.406/2002), art. 206, § 3º, V
<i>Obs: Caso o dano tenha se originado na prestação contratual, vale o prazo de 11 anos apontado acima.</i>			

<b>IV.6. Contratos e Comunicações com doadores e investidores</b>	<b>Explicação</b>		
	Documentos compartilhados com parceiros e investidores dos projetos.		
<b>Lista de Prazos</b>			
<b>Documento</b>	<b>Prazo de retenção</b>	<b>Início da contagem</b>	<b>Fundamento legal</b>
Relatórios referentes a projetos da organização (com dados anonimizados ou pseudonimizados)	Indeterminado	Após a conclusão do Projeto	Lei Geral Brasileira de Proteção de Dados (Lei nº 13.709/2018, ou LGPD), art. 15, I, II e III e art. 16
<i>Obs: Contanto que os dados contidos nos Relatórios sejam devidamente anonimizados, estes poderão ser retidos indeterminadamente pela organização (não se trata mais de dados pessoais). Caso não haja possibilidade de anonimizar por completo os dados, recomendamos que sejam pseudonimizados (ou seja, acessíveis apenas por uma chave de conhecimento do controlador). Isto ocorre, por exemplo, quando da atribuição de codinomes aos titulares que constarão nos relatórios compartilhados, enquanto a organização mantém a relação de nomes e codinomes em suas próprias bases, inacessíveis a terceiros.</i>			
Documentos de prestação de contas de Termos de Fomento e Colaboração firmados com o Poder Público	10 anos	Dia útil subsequente ao da prestação de contas	Art. 68 da Lei nº 13.019/14.
<i>Obs: As organizações têm obrigação legal de reter os documentos relacionados à prestação de contas (inclusive em plataforma digital pública) por 10 (dez) anos. No entanto, ressaltamos que as organizações poderão reter os documentos em interesse legítimo e/ou para exercício regular de direitos em eventual processo, a seu critério, por períodos maiores, contanto que os titulares dos dados documentados.</i>			