



POLÍTICA DE DADOS PESSOAIS

1. Apresentação

Nossa Empresa (a "Empresa" ou a "FLUMAR") e sua liderança estamos fortemente comprometidos em cumprir e fazer cumprir a legislação brasileira sobre Tratamento (o "Tratamento") de Dados Pessoais (os "Dados Pessoais"; no singular, o "Dado Pessoal"), notadamente a Lei Geral de Proteção de Dados (a "LGPD"), em garantir a privacidade dos Titulares (os "Titulares"; no singular, o "Titular") e em propiciar segurança e proteção razoáveis aos Dados Pessoais que tratamos.

Podemos tratar Dados Pessoais de nossos Colaboradores (os "Colaboradores"), de Pessoas Relacionadas (as "Pessoas Relacionadas"; no singular, a "Pessoa Relacionada") e de outros indivíduos para uma variedade de propósitos, inclusive legais, regulatórios e comerciais.

Esta **Política** (a "**Política**") descreve como agimos para proteger os Dados que tratamos e para garantir que os Colaboradores e as Pessoas Relacionadas entendam as diretrizes de utilização dos Dados que acessam para suas atividades legítimas de emprego ou trabalho.

A **Política** exige que Colaboradores e Pessoas Relacionadas garantam que nosso Encarregado de Dados ou DPO (o "Encarregado de Dados" ou o "DPO") seja mantido atualizado e seja consultado antes que uma nova atividade significativa de Tratamento de Dados seja iniciada, de modo a certificar que as etapas de Conformidade (a "Conformidade") relevantes sejam consideradas.

Esta **Política** foi atestada e aprovada pela alta liderança da FLUMAR e deve entrar em vigor assim que internamente divulgada. Nossa liderança está também empenhada na implementação desta **Política**, e espera que todos compartilhem desse compromisso. Queremos que qualquer um se sinta confortável em compartilhar seus Dados Pessoais conosco, e faremos nosso melhor para resolver um problema que possa surgir em relação a isso.

Qualquer Violação (a "Violação") desta **Política** é levada muito a sério, e pode resultar em Penalidades (as "Penalidades"; no singular, a "Penalidade") legais, disciplinares e contratuais.

2. Alcance e Aplicação

Esta **Política de Dados Pessoais** alcança:



- Todas as áreas da FLUMAR;
- Todas as atividades, negócios e serviços da Empresa;
- Todos os Dados Pessoais tratados em conexão com a FLUMAR;
- Todos os Dados coletados e tratados no Brasil pela FLUMAR;
- Todos os Tratamentos de Dados Pessoais, incluindo aqueles
 - Total ou parcialmente automatizados - via computador, aplicativo ou outro sistema digital);
 - Por outros meios - registros em meio físico - que integram um sistema de arquivamento.

A **Política** se aplica:



A todos os nossos Colaboradores, incluindo administradores, diretores, executivos, investidores, sócios, consultores, assessores, auditores, clientes, parceiros, ocupantes de cargos de gestão ou de confiança, empregados, contratados, terceirizados, *trainees*, estagiários, fornecedores e prestadores, e às Pessoas Relacionadas que interagem conosco, ou que atuam para nós ou em nosso nome, ou que conosco tenham um contrato ou um acordo comercial.

Nosso DPO é o responsável imediato pela implementação desta **Política**. Qualquer interessado pode manter contato com ele para esclarecimentos sobre a **Política** e seus termos.

Com base nos princípios da transparência e responsabilidade, e em respeito à Governança (a "Governança") e à Conformidade, contamos com uma Consultoria Legal (a "Consultoria Legal") independente, a quem cabe analisar questões sobre a LGPD, Dados Pessoais e seu Tratamento, orientando-nos e aconselhando-nos em nossas ações, decisões e procedimentos.

3. Propósito e Princípios

O propósito desta **Política** é fornecer diretrizes e orientações sobre o Tratamento e a proteção de Dados Pessoais, o que se aplica aos Dados: (i) tratados pela FLUMAR em suas atividades, negócios e serviços; (ii) armazenados pela FLUMAR ; e (iii) utilizados pela FLUMAR.

É essencial que nossos Colaboradores e Pessoas Relacionadas observem e coloquem em prática os princípios de proteção de Dados Pessoais abaixo:



10 PRINCÍPIOS PARA O TRATAMENTO DE DADOS PESSOAIS

FINALIDADE Todo Tratamento deve ser para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de Tratamento posterior de forma incompatível com essas Finalidades	ADEQUAÇÃO Todo tratamento deve estar de acordo com as finalidades informadas ao Titular e com o contexto do Tratamento
NECESSIDADE Todo Tratamento deve ser limitado ao mínimo necessário para a finalidade, com abrangência dos Dados pertinentes, proporcionais e não excessivos em relação à Finalidade	LIVRE ACESSO Todo tratamento deve garantir aos Titulares a consulta facilitada e gratuita sobre a forma e duração do Tratamento, bem como sobre a integralidade de seus Dados Pessoais
QUALIDADE DOS DADOS Todo Tratamento deve dar garantia, aos Titulares, de exatidão, clareza, relevância e atualização dos Dados, de acordo com a necessidade da Finalidade	TRANSPARÊNCIA Todo Tratamento deve dar 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 Todo Tratamento deve utilizar medidas técnicas e administrativas para proteger os Dados Pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão	PREVENÇÃO Todo Tratamento deve adotar medidas para prevenir a ocorrência de danos em virtude do Tratamento
NÃO DISCRIMINAÇÃO Todo tratamento deve estar configurado para que não haja manejo de Dados Pessoais para fins discriminatórios ilícitos ou abusivos	RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS Todo Tratamento deve demonstrar a 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

4. Procedimentos

4.1. Tratamento

Tratamento, na Lei Geral de Proteção de Dados, é

“toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, tratamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”.

Devemos tratar os Dados Pessoais de maneira justa, segura e lícita, respeitando os direitos dos Titulares e esta **Política**, conforme o processo abaixo:



Cada processo de Tratamento deve responder objetivamente ao seguinte:

PROCESSO DE TRATAMENTO DE DADOS PESSOAIS



1

Que processos
da área
dependem de
Dados
Pessoais?



2

Qual a
Finalidade do
Tratamento?



3

Que Dados
Pessoais
precisam ser
tratados?



4

Quais os
Dados
essenciais
para a
Finalidade?



5

Qual a Base
Legal para o
Tratamento
dos Dados?

4.2. Dados Pessoais

Basicamente, há duas categorias principais de Dados Pessoais:

- **Comuns** (os "Dados Comuns"; no singular, o "Dado Comum");
- **Sensíveis** (os "Dados Sensíveis"; no singular, o "Dado Sensível").

Dados **Comuns** são os que identificam (ou ajudam a identificar) uma pessoa **física**, mas sem avançar em sua privacidade ou comprometer sua intimidade.

Esses Dados Comuns são, por exemplo: nome, endereço, CPF, passaporte, filiação, profissão, *email*, telefone, local de trabalho, naturalidade, CNH, idade, nacionalidade e similares. São chamados "Comuns" porque, em geral, todas as pessoas os têm e porque não se referem a uma condição íntima que precisa ser especialmente protegida.

Já os Dados **Sensíveis** exprimem elementos, registros ou referências que têm relação mais estreita com a privacidade e a intimidade de um indivíduo.

Nessa categoria estão os Dados relacionados à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, à saúde, à vida sexual, à genética ou à biometria.

Além dessa divisão em categorias principais, os Dados Pessoais também podem ser diretos ou indiretos. Os diretos identificam uma pessoa sem necessitar de outros elementos (exs.: nome e CPF); os indiretos precisam de outros Dados para identificar uma pessoa (exs.: filiação e profissão).

Todo Tratamento de Dados exige pelo menos uma Finalidade e uma Base Legal permitida pela LGPD (v. mais sobre Finalidade e Base Legal nesta **Política**).

Há Bases Legais específicas para Tratamento de Dados Comuns, e outras para tratar Dados Sensíveis. Por exemplo: a Base Legal do Interesse Legítimo (o "Interesse Legítimo") pode ser utilizada para tratar Dados Comuns, mas **não** para tratar Dados Sensíveis.

Por fim, lembre-se de que, quando esta **Política** fala em Dados Pessoais, está se referindo a Dados de pessoas **físicas** (indivíduos naturais). Isso quer dizer que a **Política não alcança** dados de pessoas **jurídicas** (exs.: CNPJ, endereço, razão social, etc.).

4.3. Finalidade

A Finalidade (a "Finalidade") do Tratamento de Dados Pessoais é uma exigência da Lei Geral de Proteção de Dados (art. 6º, I).

Finalidade é responder: *por que (para que)* se faz o Tratamento de Dados Pessoais?



Exemplo: se a Empresa quer contratar um novo empregado, a área de RH vai precisar dos Dados Pessoais dele.

Assim, a Finalidade do Tratamento é “contratar um empregado”.

Outro exemplo: a área comercial quer fazer contrato com um Cliente. Também nesse caso ela vai precisar dos Dados Pessoais dos representantes do Cliente.

Portanto, a Finalidade do Tratamento é “concluir um contrato”.

Podemos tratar Dados Pessoais para diferentes Finalidades, tais como:



- Adequar produtos e serviços disponibilizados pela FLUMAR; Aprimorar
- nossa comunicação externa e interna; Combater fraude e violação de
- direitos; Cumprir obrigações legais ou regulatórias e exercer direitos
- em demandas judiciais, administrativas ou arbitrais; Elaborar perfis de
- Clientes a partir de Dados fornecidos e operações realizadas, a fim de
- personalizar serviços, produtos e benefícios; Identificar e autenticar
- Clientes e administrar e processar pedidos e
- cadastros para cumprir obrigações pelo uso de nossos serviços e da
- compra de bens e serviços; Informar aos Clientes sobre novidades,
- produtos, serviços, conteúdos, funcionalidades, promoções, notícias e
- eventos; Propiciar um Propósito Negocial (o "Propósito Negocial").
-

A Finalidade, na prática, "justifica" o Tratamento dos Dados. Ou seja, quem trata Dados deve ter uma "justificativa" (Finalidade) para isso.

4.4. Base Legal

Base Legal é o nome dado a cada uma das hipóteses em que o Tratamento de Dados Pessoais é permitido pela LGPD.

Para chegar a uma Base Legal confiável para um Tratamento responda:

- Sei exatamente qual é a Finalidade do Tratamento?
- Sei de quais Dados necessito?
- Consigo limitar o Tratamento apenas a Dados essenciais?
- Posso chegar à Finalidade sem tratar esses Dados?
- Sou capaz de parar o Tratamento a qualquer instante, se necessário?
- Estou em posição de poder sobre o Titular (ex.: sou o "chefe" dele)?

É possível utilizar qualquer Base Legal, mas é necessário confiar naquela que **melhor** se encaixa na Finalidade, *não na Base que é mais cômoda*.

Conforme a LGPD, apenas as Bases Legais abaixo podem ser aplicadas ao Tratamento de Dados Pessoais **Comuns** (válido para organizações privadas):



Para o Tratamento de Dados Pessoais **Sensíveis** aplicam-se somente as Bases Legais adiante (válido para organizações privadas):



É importante saber: se ao menos uma Base Legal não puder ser aplicada a um Tratamento, isso pode ser sinal de que esse Tratamento pode não estar conforme à LGPD ou ser considerado irregular e até ilegal.

Isso pode trazer consequências para a Empresa e para os Agentes que fizeram o Tratamento não conforme, irregular ou ilegal.

4.5. Interesse Legítimo

Se o Tratamento de Dados Pessoais é necessário ou indispensável, mas nenhuma outra Base Legal permitida pela LGPD se aplica ao caso concreto, talvez seja possível utilizar a Base Legal do **Interesse Legítimo**.

Essa Base é diferente das outras, já que não se concentra em uma Finalidade específica e não se refere a um Tratamento com o qual o Titular já tenha concordado. O Interesse Legítimo tem mais flexibilidade (*mas não muita*), e em princípio pode ser aplicado a variados Tratamentos, desde que tenham Finalidade convincente e bem descrita.

Isso significa que não se pode aplicar o Interesse Legítimo para qualquer Tratamento, de maneira indiscriminada. Fazer isso gera riscos ao Titular e à FLUMAR.

Para que o Interesse Legítimo possa ser bem aplicado, o Agente de Tratamento deve fazer um teste. É o teste FINE: **F**inalidade, **N**ecessidade e **E**quilíbrio.

Nesse tipo de teste, é preciso perguntar;

- **FINALIDADE:** existe mesmo um Interesse Legítimo por trás do Tratamento desejado?
- **NECESSIDADE:** o Tratamento pretendido é de fato necessário?
- **EQUILÍBRIO:** é certo dizer que o Interesse Legítimo utilizado não ofende direitos, interesses ou liberdades do Titular?

Mas utilizar o Interesse Legítimo também pode exigir, por solicitação do DPO, uma Avaliação de Interesse Legítimo (a "Avaliação de Interesse Legítimo" ou a "LIA"). Nesse documento, o Agente de Tratamento (o "Agente de Tratamento"; no plural, os "Agentes de Tratamento") justifica por que escolheu o Interesse Legítimo como Base Legal.

De qualquer modo, sempre há uma Base Legal para o Tratamento desejado. **O Interesse Legítimo é apenas uma delas** - lembre-se disso.

Se você não sabe quando utilizar uma LIA, ou como fazê-la, peça ajuda ao DPO.

4.6. Consentimento

O Tratamento de Dados Pessoais depende de uma Finalidade, de uma Base Legal (autorizada pela LGPD) e da aplicação desta **Política**.

Entre as Bases Legais autorizadas pela LGPD está o **Consentimento** (o "Consentimento").

Basicamente, Consentimento é uma concordância prévia e escrita que o Titular dá para que seus Dados Pessoais sejam tratados. Funciona, na prática, como permissão do Titular ao Tratamento de seus Dados, endereçada ao Agente de Tratamento (Controlador ou Operador).

No entanto, essa Base traz muitos desafios, e por isso é a menos aplicada.

Um dos desafios é que, mesmo que o Consentimento seja obrigatório em certas situações, pode ser revogado a qualquer momento pelo Titular, o que gera problemas para o Tratamento dos Dados, especialmente se são essenciais para uma Finalidade.

Outro desafio é que o Consentimento só cabe em Finalidades muito específicas, estabelecidas antes do início do Tratamento, sem possibilidade de alteração posterior. Se for feita uma alteração na Finalidade, outro Consentimento deve ser solicitado ao Titular.

Portanto, tenha sempre isso em mente se precisar utilizar o Consentimento como Base Legal para tratar Dados Pessoais.

Um Consentimento pode ser necessário se:

- For preciso tratar imagens do Titular para fins comerciais ou financeiros;
- Há razoáveis dúvidas sobre se o Titular concorda com o Tratamento de seus Dados;
- O Tratamento pode trazer alto risco de exposição para o Titular.

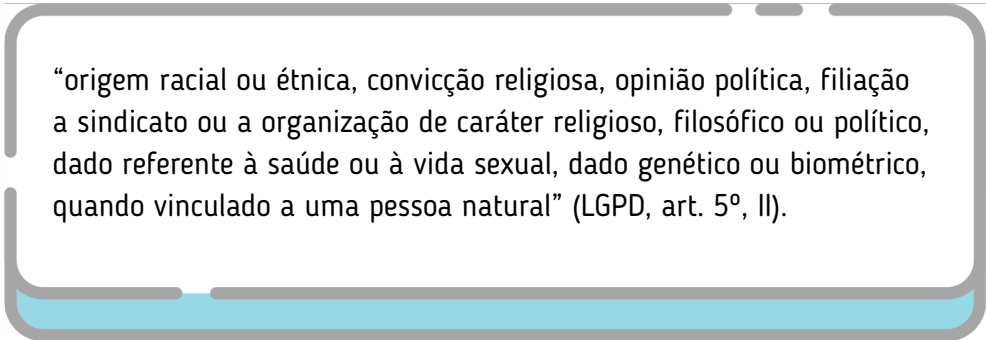
E um Consentimento é obrigatório se:

- Há Tratamento de Dados Pessoais de crianças;
 - Outra Base Legal não puder ser aplicada;
 - Outra razão não puder ser aplicada para uma Transferência Internacional de Dados (a "Transferência Internacional").
-

4.7. Dados Sensíveis

Todo Dado Pessoal tem caráter confidencial e "sensível", no sentido de que sua má utilização ou Tratamento ilegal ou irregular pode trazer prejuízos ao Titular.

Mas há uma categoria de Dados reconhecida pela LGPD como particularmente Sensível: são os que se referem a pessoas mais vulneráveis (carentes de maior proteção) ou que se relacionam a aspectos fortemente íntimos e reservados de um indivíduo. Eles têm a ver com



“origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (LGPD, art. 5º, II).

Essa categoria pode criar riscos mais significativos para os direitos e liberdades fundamentais de uma pessoa (ex.: discriminação, *bullying* ou *stalking*). Por isso, *Dados Sensíveis só devem ser tratados quando há evidente necessidade, se são indispensáveis para uma Finalidade e sempre sob uma Base Legal específica para eles.*

Mas é bom saber que a Base Legal do Interesse Legítimo **não** pode ser utilizada para o Tratamento de Dados Sensíveis.

A condição para Tratamento de Dados Pessoais Sensíveis é a estrita obediência à LGPD. Se não há uma Finalidade e uma Base Legal específica para isso, o Tratamento **não** deve ser iniciado, **deve** ser interrompido ou **precisa ser** ajustado.

Em alguns casos, a FLUMAR pode tratar Dados Sensíveis, especialmente para cumprir obrigações legais e regulatórias, garantir a integridade e a segurança no trabalho, manter registros de saúde e propiciar benefícios legais e regulamentares a seus empregados.

Mas tomamos medidas e precauções adicionais em relação a esses Dados, e os mantemos sob rígidos protocolos de controle e segurança.

Sobre esse assunto, consulte nosso DPO e nosso *head* de Recursos Humanos.

4.8. Controle Centralizado

Manter um **Controle Centralizado** (o "Controle Centralizado") do Tratamento de Dados Pessoais é outra exigência da LGPD (art. 37) e obrigação de todos os Agentes de Tratamento.

Agente de Tratamento pode ser o Controlador - aquele que dá as ordens e orientações sobre o Tratamento de Dados Pessoais - ou o Operador (o "Operador") - aquele que trata Dados sob as ordens e orientações do Controlador.

Em nosso caso, a FLUMAR é uma Controladora de Dados Pessoais, e cabe a ela estabelecer as ordens, normas, controles e orientações para tratar e dar segurança a esses Dados. Nesse sentido, a FLUMAR é Controladora *principal* dos Dados.

Mas há outro tipo de Controlador: o *derivado*. Esse Controlador é o Colaborador que, na sua área, trata Dados Pessoais, ou a Pessoa Relacionada que, ao interagir conosco, trata Dados Pessoais. Por isso, tanto a FLUMAR é Controladora de Dados Pessoais de seus Colaboradores, quanto cada Colaborador é um Controlador dos Dados que trata para suas atividades.

Cabe aos Controladores (principal e derivado) manter um registro dos Dados que tratam e dos Tratamentos que fazem. E cada área de nossa Empresa, por seu gestor, precisa fazer seu Registro Individual (o "Registro Individual").

Podemos realizar, a qualquer momento, uma Avaliação de Conformidade em um Operador que atua sobre nossas diretrizes e orientações para saber se ele está seguindo os processos e instruções por nós estabelecidos nesta **Política** e em outros instrumentos.

Para ajuda sobre o Registro Individual, consulte nosso DPO.

4.9. Documentação

Tratar Dados Pessoais com foco na redução de riscos exige compromisso com os princípios do Capítulo 3 e uma **Documentação** adequada (a "Documentação").

Documentar é mostrar, a partir de evidências (registros, controles, etc.), que o Tratamento dos Dados tem uma Finalidade, uma Base Legal e que está conforme à LGPD.

Devemos garantir que pessoas cujos Dados estão sendo tratados pela FLUMAR possam ser esclarecidas, se elas pedirem, sobre a Finalidade de um Tratamento e sobre a Base Legal escolhida para executá-lo.

O esclarecimento, quando tiver de ser prestado, deve ser feito de forma direta e objetiva, em linguagem compreensível.

Para dúvidas sobre isso, busque ajuda de nosso DPO.

4.10. Cookies

Cookies (os "Cookies") são pequenos arquivos que podem ser baixados diretamente em um dispositivo quando alguém acessa, usa ou navega por uma página na *Internet*, inclusive a nossa.

Eles permitem que o *site* reconheça o dispositivo e armazene elementos sobre preferências ou histórico de navegação. Além disso, facilitam a navegação, aumentam a usabilidade de *sites* e aplicativos e ajudam a identificar as seções mais populares do *site* visitado.

É possível que alguns Dados Pessoais sejam salvos em Cookies, desde que a pessoa tenha concordado com isso quando configurou seu navegador. Isso pode facilitar o acesso *online* seguro para que não seja preciso inserir o ID de usuário e senha a cada visita.

Quando alguém acessa determinada página, inclusive a nossa, e continua a navegar por ela, entende-se que aceita o uso de Cookies. Mas é claro que a pessoa pode revogar essa aceitação a qualquer instante, ou gerenciar os Cookies utilizados em cada *site*.

Quando utilizamos Cookies, o fazemos com vistas a registrar as preferências de nossos usuários e otimizar o *design* de nosso *site*. Isso nos dá a chance de fornecer um conteúdo mais adequado às necessidades dos interessados e, a partir daí, melhorar nossos serviços, produtos, divulgações e relacionamentos, tudo sob procedimentos estritamente lícitos e transparentes.

Se alguém optar por não aceitar Cookies, ainda pode acessar e usar nosso *site*. E pode impedir que Cookies sejam armazenados em seu dispositivo, configurando seu navegador para isso, ou excluir os Cookies que já estejam no dispositivo. Mas lembramos que, se alguém optar por não

aceitar Cookies estritamente necessários para os serviços fornecidos por nosso *site* ou plataformas, isso pode resultar em disponibilidade reduzida ou menor funcionalidade desses serviços. Também recomendamos que, ao visitar uma página, a

pessoa observe com atenção as condições

dos *banners* de Cookies, um aviso frequentemente exibido na primeira visita de um usuário a um *site* informando-o sobre os Cookies e rastreadores que o *site* utiliza e solicitando permissão do usuário para armazená-los em seus dispositivos.

Para saber mais sobre Cookies, incluindo sobre quais foram definidos e como gerenciá-los ou excluí-los, visite www.aboutcookies.org ou www.allaboutcookies.org.

4.11. Deveres

Nossos deveres:

a) Da Organização:



- Adotar ações para que os Dados e seus Tratamentos sejam mapeados, registrados, controlados e realizados sob as normas da LGPD;
- Adotar medidas para Armazenamento seguro dos Dados Pessoais;
- Assegurar que Colaboradores e Pessoas Relacionadas cumpram esta **Política** e as normas da ANPD;
- Avaliar os riscos que podem ser gerados se os Dados forem comprometidos;
- Determinar que cada Tratamento tenha Finalidade e Base Legal;
- Disseminar conhecimento sobre esta **Política**;
- Garantir que os procedimentos de Tratamento sejam estritamente legais;
- Implementar e revisar ações e procedimentos sobre Incidentes de Segurança (os "Incidentes de Segurança"; no singular, o "Incidente de Segurança");
- Implementar esta **Política**, mantê-la atualizada e divulgá-la internamente;
- Manter atualizados os processos para Tratamento de Dados Pessoais.

b) Dos Colaboradores e Pessoas Relacionadas (as "Pessoas Relacionadas"; no singular, a "Pessoa Relacionada"):



- Determinar a Finalidade do Tratamento e estabelecer sua Base Legal; Documentar
- seus processos de Tratamento de Dados Pessoais; Jamais reter ou armazenar
- Dados além do período necessário; Jamais armazenar Dados incorretamente, ser
- descuidado com eles ou nos fazer
- violar, por suas ações, as leis de proteção de Dados e nossas políticas;
- Jamais usar Dados Pessoais de forma displicente, ilegal, irregular ou para
- objetivos ilícitos ou particulares;
- Levantar, sem demora, qualquer preocupação, notificar Incidentes ou erros e
- relatar ações suspeitas ou contrárias a esta **Política**;
- Não tratar Dados Sensíveis se não for indispensável;
- Não tratar mais Dados que o necessário;
- Tratar apenas os Dados mínimos e essenciais para a Finalidade;
- Verificar continuamente se as atividades de Tratamento de Dados que
- executam cumprem nossas políticas e se são lícitas e justificadas.

c) Do DPO:



- Aceitar reclamações e comunicações dos Titulares de Dados, prestar esclarecimentos e adotar providências;
- Manter a alta administração atualizada sobre estado, progresso (ou retrocesso), riscos, incidentes, maus hábitos, práticas e problemas relacionados a esta Política;
- Manter estreita relação com os consultores legais sobre esta Política e as matérias relacionadas à função de DPO e ao Tratamento de Dados;
- Manter-se atualizado sobre a legislação e temas pertinentes à proteção de Dados;
- Monitorar o cumprimento da legislação de proteção de Dados e desta Política;
- Organizar ações de disseminação de conhecimento em proteção de Dados Pessoais;
- Orientar Colaboradores e Pessoas Relacionadas da Empresa a respeito das práticas a serem adotadas e da proteção de Dados Pessoais;
- Receber comunicações da ANPD e adotar providências;
- Responder a perguntas sobre proteção de Dados Pessoais;
- Revisar, sempre que necessário, as Políticas e os procedimentos de proteção de Dados.

d) Da área ou gerência de tecnologia da informação:



- Apoiar o DPO e os Agentes de Tratamento de Dados da FLUMAR;
- Apresentar sugestões de aprimoramento de controles para proteção de Dados;
- Avaliar e corrigir vulnerabilidades de sistema;
- Garantir que sistemas, serviços, softwares e equipamentos atendam aos padrões de segurança aceitáveis;
- Verificar regularmente hardwares e softwares de segurança para garantir que funcionem corretamente e que forneçam a confiabilidade que deles se espera.

e) Da área ou gerência de *marketing*:



- Agir com o DPO para que as ações de *marketing* estejam conforme a LGPD;
- Apresentar sugestões de melhoria e aprimoramento de campanhas internas para disseminação de conhecimento sobre esta **Política** e a necessidade de seu completo entendimento e cumprimento;
- Participar das declarações de proteção de Dados anexadas a *emails* voltados para assuntos de *marketing*.

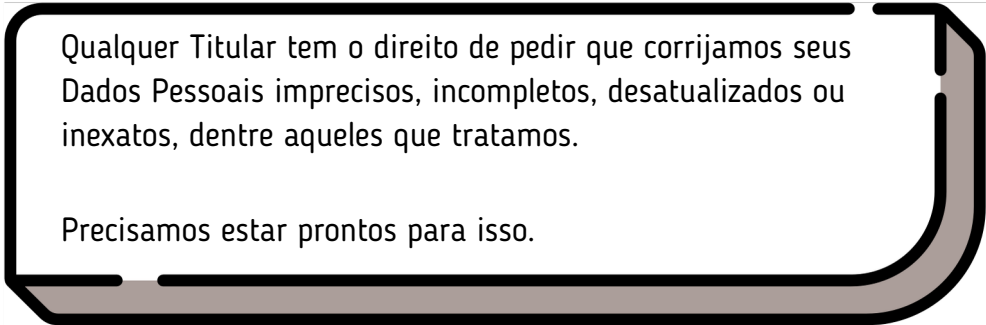
4.12. Precisão

Nossa Empresa se empenha em assegurar que os Dados Pessoais que tratamos e utilizamos sejam **precisos**, considerada a Finalidade para a qual foram pesquisados, selecionados e coletados.

Não tratamos Dados coletados sob uma Finalidade para utilizá-los em qualquer outra não conectada, salvo se o Titular dos Dados tiver concordado com isso ou de outra forma razoavelmente espere que isso ocorra.

Se um Colaborador da FLUMAR não está suficientemente seguro quanto à Finalidade para a qual os Dados foram coletados, mas precisa utilizá-los, ou quer utilizá-los para Finalidade diferente da original, deve buscar orientação prévia do DPO.

Se a Finalidade proposta for significativamente diferente, envolver a combinação de Dados de diferentes naturezas ou tiver um impacto significativo sobre o Titular, o DPO pode exigir que uma Avaliação de Impacto de Proteção de Dados (DPIA) (a "Avaliação de Impacto de Proteção de Dados" ou a "DPIA") seja previamente realizada. Nesse caso, ele pode orientar sobre como e quando fazer essa DPIA.



Qualquer Titular tem o direito de pedir que corrijamos seus Dados Pessoais imprecisos, incompletos, desatualizados ou inexatos, dentre aqueles que tratamos.

Precisamos estar prontos para isso.

Se você acredita que os Dados Pessoais que trata ou que pretende tratar podem não ser exatos, precisos, completos ou atualizados, você deve registrar essa dúvida e reportar-se imediatamente ao DPO, que o orientará como agir.

4.13. Segurança

Nós nos esforçamos para manter os Dados Pessoais que tratamos razoavelmente **seguros** contra perda e contra acesso ou utilização ilícita, indevida ou não autorizada.

Entretanto, não podemos assegurar que nossas medidas sempre funcionem, ou que sempre funcionem como esperado ou pretendido, especialmente em quadros excepcionais ou naqueles decorrentes de ataques externos fora de nosso controle, imprevisíveis ou inesperados. Nesses casos, tomaremos as medidas razoáveis ao nosso alcance, segundo o estado da técnica na época de cada evento, e faremos as comunicações exigidas pela LGPD aos Titulares e à ANPD.

Quando outras organizações tratam Dados como um serviço em nosso nome, o DPO estabelece que arranjos específicos de segurança precisam ser implementados em Contratos ou Acordos de Nível de Serviço (SLAs) com elas. Esses arranjos podem incluir cláusulas, normas adicionais, aditivos, anexos ou apêndices, inclusive para Contratos em andamento.

Em certas circunstâncias, podemos adotar padrões mínimos de segurança para proteger os Dados Pessoais, incluindo:

- Permissão de acesso a bases de Dados ou locais de armazenamento apenas a pessoas previamente autorizadas, comprometidas em manter sigilo absoluto sobre os Dados;
 - Dados em CDs, cartões de memória ou dispositivos semelhantes devem ser criptografados ou protegidos por senhas fortes, regularmente revistas e alteradas, e ser bloqueados com segurança quando não estiverem em uso;
 - Dados em meio virtual devem estar protegidos por senhas fortes, regularmente revistas e alteradas, e para isso encorajamos que todos utilizem um gerenciador de senhas;
 - Dados jamais devem ser salvos diretamente em um dispositivo móvel, como um *laptop*, *tablet* ou *smartphone*;
 - Dados impressos devem ser triturados se não forem mais necessários, se a Finalidade de seu Tratamento tiver sido alcançada ou se seu Tratamento for cancelado ou proibido ;
 - Os Dados devem estar seguros conforme os procedimentos de *backup* da FLUMAR;
 - Se os Dados estão em papel impresso, ou se o próprio documento for um Dado, devem estar em lugar seguro, sem acesso a pessoas não autorizadas;
 - Servidores que contenham Dados devem ser mantidos em ambiente seguro, longe do espaço comum da Empresa, e só devem ser acessados pelo pessoal técnico autorizado.
-

4.14. Compartilhamento e Transferência

Um **Compartilhamento de Dados** (o "Compartilhamento") pode ocorrer nos casos de:

- Cumprimento de obrigações legais, regulatórias ou regulamentares;
- Cumprimento de requisições, solicitações ou decisões de autoridades competentes;
- Identificação, prevenção e investigação de potenciais infrações ou atos ilícitos (inclusive fraude, lavagem de dinheiro e financiamento de terrorismo);
- Melhoramento da experiência do Titular com produtos e serviços oferecidos;
- Parceria com empresas relacionadas às atividades da FLUMAR;
- Prática de ações comerciais necessárias às atividades da FLUMAR;
- Proteção, defesa e exercício regular de direitos;
- Proteção dos interesses da FLUMAR em caso de litígio ou conflito;
- Transações e alterações societárias envolvendo a FLUMAR, nos casos em que a comunicação dos Dados seja necessária à continuidade dos serviços;
- Transações e atividades de execução de contrato;
- Verificação de informações cadastrais, registrais e comerciais.

O Tratamento de Dados Pessoais ocorre no Brasil, mas pode ser que, em certas circunstâncias, precisemos transferir Dados a outros países. No entanto, tomaremos medidas razoáveis para que isso ocorra conforme a LGPD e os regulamentos da ANPD.

Em geral, uma Transferência Internacional vai depender de o país receptor demonstrar grau de proteção similar ao estabelecido pela LGPD ou de uma autorização da ANPD.

Nenhum Colaborador nosso pode compartilhar ou transferir Dados Pessoais para o exterior ou para qualquer outro lugar fora das regras e procedimentos normais, sem que a FLUMAR o permita e sem prévio aval do DPO.

4.15. Retenção e Armazenamento

Nós só fazemos **Retenção** (a "Retenção") ou **Armazenamento** (o "Armazenamento") de Dados Pessoais pelo período *estritamente necessário*, e confiamos que nossos Colaboradores e Pessoas Relacionadas se comportem de igual maneira.

Dados Pessoais podem ser retidos ou armazenados para:

- Apresentar e comprovar Tratamentos em uma questão legal, judicial ou administrativa;
- Atender a pedidos de Reguladores (os "Reguladores"; no singular, o "Regulador");
- Atender a requisições de organizações agindo em nome do Titular;
- Atender a uma obrigação legal, contratual ou regulatória;
- Atender a obrigações fiscais, tributárias, trabalhistas e previdenciais;
- Compartilhar referências com autoridades legais e administrativas;
- Conservar evidências materiais;
- Manter relações de nossa organização com a sociedade;
- Obter meios de defesa judicial ou administrativa;
- Prestar esclarecimentos sobre Tratamentos;
- Responder a determinações judiciais;
- Responder a outros propósitos lícitos e relevantes.

Os prazos de Retenção e Armazenamento de Dados podem variar em função da categoria dos Dados ou das regras legais aplicáveis a cada situação, mas todos os que praticamos são corretos, justificáveis e razoáveis.

Nosso DPO deve ser consultado para garantir que um prazo de Retenção ou de Armazenamento adequado seja aplicado.

4.16. Incidente de Segurança

Incidente de Segurança é todo evento confirmado, de natureza adversa, envolvendo Dados Pessoais, que implica violação da segurança dos Dados e que pode ocasionar risco ou dano relevante ao Titular.

Um Incidente de Segurança pode ser um acesso ou uma divulgação não autorizada, acidental ou ilícita, com destruição, perda, alteração, vazamento ou Tratamento inadequado ou ilícito de qualquer Dado Pessoal.

Todo Incidente deve ser imediatamente informado ao DPO da FLUMAR, a quem cabe comunicar o fato à ANPD com a maior urgência possível e tomar medidas necessárias.

Da comunicação à ANPD devem constar:

- Natureza dos Dados atingidos;
- Informações sobre os Titulares envolvidos;
- Indicação das medidas técnicas e de segurança utilizadas para proteção dos Dados (observados os segredos comercial e industrial);
- Riscos relacionados ao Incidente;
- Motivos da demora, se a comunicação não foi imediata;
- Medidas que foram ou serão adotadas para reverter ou mitigar os efeitos do Incidente.

Se um Colaborador ou Pessoa Relacionada tiver evidentes suspeitas de que um Incidente de Segurança ocorreu, está ocorrendo ou está prestes a ocorrer, tem o dever de informar nosso DPO sem demora sobre isso.

Ocultar um Incidente de Segurança, ou deixar de informá-lo ao DPO, pode resultar em Penalidades Disciplinares a quem o ocultou, ou não o informou, além de sanções contratuais.

4.17. Término do Tratamento

Como todo processo, o Tratamento de Dados Pessoais tem início, meio e fim.

A Lei Geral de Proteção de Dados prevê que o Término do Tratamento de Dados (o "Término do Tratamento") pode ocorrer se:

- A Finalidade foi alcançada;
- Os Dados deixaram de ser necessários ou pertinentes para a Finalidade;
- O período de Tratamento chegou ao fim;
- O Titular revogou seu Consentimento;
- O Titular solicitou o término do Tratamento;
- Há determinação da ANPD, no caso de violação da LGPD;
- O Controlador assim decidir.

Findo o Tratamento, o Agente deve eliminar os Dados (ou restituí-los ao Titular, se receber uma solicitação escrita nesse sentido).

Mesmo com o Término do Tratamento, os Dados ainda podem ser mantidos pelo Controlador nas seguintes hipóteses:

- Cumprimento de obrigação legal ou regulatória pelo Controlador;
 - Estudo por órgão de pesquisa (garantida, sempre que possível, a Anonimização);
 - Transferência a terceiro, respeitados os requisitos de Tratamento da LGPD;
 - Uso exclusivo do Controlador, sem acesso por terceiro, desde que anonimizados.
-

5. Direitos dos Titulares

Os Titulares de Dados Pessoais têm direitos sobre seus Dados que devemos cumprir.

Conforme a LGPD (arts. 18 e 20), os Titulares têm direito de:



- Acesso aos Dados (obtenção de cópia);
- Anonimização, bloqueio ou eliminação de Dados Pessoais desnecessários, excessivos ou tratados em desconformidade com a Lei Geral de Proteção de Dados;
- Apresentar reclamação à Autoridade Nacional de Proteção de Dados;
- Confirmação da existência de Tratamento;
- Correção de Dados incompletos, inexatos ou desatualizados;
- Eliminação dos Dados Pessoais tratados sem seu Consentimento (nos casos em que o Consentimento é necessário);
- Oposição (a "Oposição") ao Tratamento;
- Portabilidade (a "Portabilidade") dos Dados Pessoais a outro Controlador, mediante requisição expressa;
- Possibilidade de não fornecer Consentimento para Tratamento e de obter esclarecimentos sobre as consequências da recusa;
- Referências sobre as organizações com as quais seus Dados foram compartilhados ou para as quais foram transferidos;
- Revisão de decisões que foram baseadas apenas em Tratamento Automatizado de Dados (o "Tratamento Automatizado de Dados") que afetem seus direitos;
- Revogação do Consentimento.

6. Acesso e Portabilidade

Outro dos direitos que a LGPD dá ao Titular é o controle sobre seus Dados Pessoais. Isso ajuda o Titular a entender como e por que estamos utilizando seus Dados e a verificar se estamos fazendo isso de forma legal.

Esse direito inclui a confirmação de que os Dados estão em tratamento, de ter **Acesso** (o "Acesso") a eles e de solicitar sua **Portabilidade** para outro Controlador. Isso pode ser atendido conforme as regras abaixo.

Para o pedido de Acesso:

- Se o Titular fizer uma requisição de Acesso, devemos fornecer-lhe gratuitamente uma cópia dos seus Dados que tratamos; um prazo aceitável é trinta dias, a contar do primeiro dia útil seguinte àquele em que a requisição foi recebida;
- Devemos nos esforçar para fornecer ao Titular Acesso aos Dados em formato eletrônico;
- Se o cumprimento da requisição for complexo, o prazo pode ser prorrogado por mais trinta dias consecutivos, mas o Titular deve ser avisado nos primeiros trinta dias;
- Podemos nos recusar a responder a certas requisições, e, no caso de circunstâncias infundadas ou excessivas, cobrar uma taxa justa;
- Se a requisição alcançar grande quantidade de Dados, podemos solicitar que o Titular especifique os de que prioritariamente precisa;
- Nenhum dos Dados pode ser alterado após o recebimento da requisição.

No caso de Portabilidade:

- Devemos nos esforçar para fornecer os Dados em formato estruturado comumente utilizado, legível por máquina, como um arquivo CSV (*Comma-Separated Values*);
 - Devemos fornecer os Dados ao Titular ou ao Controlador a quem o Titular quer transferi-los (nesse último caso o Titular nos deve apresentar uma autorização pessoal);
 - Isso deve ser feito gratuitamente e no máximo em trinta dias, prazo que pode ser estendido para até sessenta dias, no caso de solicitações complexas ou numerosas, mas o Titular deve ser informado disso nos primeiros trinta dias.
-

7. Aviso de Privacidade

Aviso de Privacidade é o documento que a Empresa coloca à disposição de seu público (interno e externo) para informar aos Titulares como seus Dados são coletados, tratados, armazenados, utilizados e destinados.

Sempre que houver coleta de Dados é recomendável informar que a FLUMAR tem seu Aviso de Privacidade e onde ele pode ser acessado.

Um Aviso de Privacidade deve ser claro, escrito em linguagem direta e em geral contém:

- As Bases Legais que podemos utilizar;
 - As categorias de Dados abrangidas;
 - As finalidades usuais do Tratamento;
 - Esclarecimentos sobre Transferências Internacionais;
 - Identificação e contato do Controlador e do DPO;
 - O direito de apresentar uma Reclamação à ANPD;
 - O direito de utilizar procedimentos internos de reclamação e solicitação;
 - Retenção dos Dados;
 - Se os Dados são atualizados espontaneamente ou não;
 - Se são compartilháveis e com quem.
-

8. Terceiros

Na qualidade de Controladora de Dados Pessoais (LGPD, art. 5º, VI), qualquer Contrato (o "Contrato") com **terceiros** em que sejamos parte e que envolva Tratamento de Dados Pessoais deve ser adequadamente formalizado (assinado e registrado).

Esses contratos devem conter cláusulas sobre:

- Atuação em solicitações para que os Titulares exerçam seus direitos;
- Averiguação de Conformidade (a "Averiguação de Conformidade");
- Compartilhamento (se pode ocorrer ou não);
- Definição sobre quem é Controlador e Operador;
- Destinação dos Dados quando a Finalidade é cumprida;
- Limites do Tratamento;
- Os Dados tratados;
- Proteção dos Dados em Incidentes de Segurança;
- Respostas a Titulares, à ANPD e a terceiros;
- Transferência Internacional.

So devemos nomear e contratar terceiros que possam oferecer garantias certas e adequadas, conforme a LGPD (e também o GDPR, em determinados casos), de que os direitos dos Titulares vão ser respeitados e protegidos.

Caso sejamos um Operador de Dados Pessoais, devemos agir exclusivamente sob instruções documentadas do Controlador.

9. Monitoramento e Treinamento

Periodicamente, podemos realizar uma **Verificação de Conformidade** (a "Verificação de Conformidade") relacionada aos Dados Pessoais que cada área nossa trata.

Esse procedimento pode incluir avaliações críticas sobre que Dados são armazenados, como e onde o são, como são utilizados, quem é o responsável pelos Tratamentos, os períodos de Retenção e outros elementos igualmente relevantes.

Independentemente disso, cada Agente de Tratamento pode realizar sua própria Verificação de Conformidade, utilizando o modelo e o cronograma que o Encarregado de Dados vai elaborar, divulgar e acompanhar.

Nosso DPO é responsável por monitorar a aplicação desta **Política**, mas cabe a cada um cumpri-la e notificar o DPO sobre qualquer Violação de seus termos.

Nossos Colaboradores recebem **treinamento** apropriado sobre as disposições da legislação de proteção de Dados específicas ~~para o seu papel~~. Cada um deles deve completar todo o treinamento que lhe for solicitado pelo DPO. Se a posição funcional ou responsabilidades de um

Colaborador da FLUMAR for alterada, ele é o responsável por solicitar novos treinamentos apropriados de proteção de Dados relevantes para sua nova função ou responsabilidades.

10. Notificação de Violação

Qualquer pessoa pode relatar uma **Violação** desta **Política** ou da legislação de proteção de Dados Pessoais, e isso deve ser feito o mais rapidamente possível.

Nossos Colaboradores e Pessoas Relacionadas têm a obrigação de relatar falhas reais ou potenciais de Conformidade relacionadas à proteção de Dados Pessoais.

A análise dessas falhas nos permite:

- Avaliar sua extensão e efeitos;
- Investigá-las e tomar medidas corretivas, se necessário;
- Manter um registro regular dos eventos;
- Notificar a ANPD de uma falha de conformidade material ou como parte de um padrão.

Todo Colaborador ou Pessoa Relacionada, ou qualquer um que interage com a FLUMAR em virtude de um contrato ou de um interesse comum, que não notificar um Incidente de Segurança, uma Violação ou ameaça de Violação, ou que, mesmo constatando, conhecendo ou suspeitando de um Incidente ou Violação, não seguir os procedimentos corretos de notificação, pode ser submetido a penalidades legais, disciplinares e contratuais apropriadas.

11. Accountability e Transparência

Devemos estar prontos para garantir a prestação de contas (**accountability**) e a transparência em qualquer operação de Tratamento de Dados Pessoais.

A legislação de proteção de Dados obriga que todos assumam uma abordagem proativa para a segurança de Dados.

A fim de incentivar as melhores práticas – e evitar penalidades e outras consequências –, Colaboradores e Pessoas Relacionadas devem ler, entender e compreender esta **Política** e colocá-la em prática no dia a dia.

Aos Colaboradores cabe tratar os Dados Pessoais uns dos outros com permanente cuidado, legitimidade e consideração, de forma a garantir que a FLUMAR seja capaz de demonstrar Conformidade também nesse caso.

12. Normas Gerais

Podemos atualizar ou alterar esta **Política** a qualquer momento, inclusive se a legislação brasileira mudar, mas sempre publicaremos outra versão dela se fizermos atualizações ou alterações substanciais.

Sempre que necessário, podem ser editadas normas corporativas complementares para auxiliar o bom cumprimento desta **Política**.

Recomendamos que todos verifiquem esta **Política** regularmente para que se mantenham atualizados quanto a seus termos e condições.

Esta **Política** é redigida em Português do Brasil, mas admite traduções para outros idiomas. Em todo caso, o idioma que prevalece é o Português do Brasil, considerando-se os demais apenas como referência linguística.

Qualquer referência feita nesta **Política** a uma cláusula, item ou anexo deve ser entendida como menção a cláusula, item ou anexo da própria **Política**, salvo expressa previsão em contrário. O significado atribuído a cada termo ou expressão definido no item **15** deve ser igualmente aplicável nas formas singular e plural desse termo ou expressão, e as palavras indicativas de gênero incluem ambos os gêneros (feminino e masculino).

Os termos “incluir”, “inclui”, “inclusive” ou “incluindo”, empregados nesta **Política**, devem ser interpretados como sendo sucedidos pela expressão “sem limitação”.

Toda referência a leis, decretos e outros normativos pressupõe o texto da lei, decreto ou normativo em vigor no momento e toda a legislação complementar relacionada.

13. Contato e Reclamações

Se um Colaborador ou Pessoa Relacionada tiver dúvida sobre esta **Política** ou sobre como lidamos com Dados Pessoais, inclusive os seus próprios, pode falar conosco no endereço lgpd@flumar.com.br.

E qualquer Colaborador ou Pessoa relacionada também pode fazer contato com nosso DPO no endereço dpo@flumar.com.br.

Além disso, todo Titular de Dados Pessoais tem direito de fazer uma Reclamação (a "Reclamação") à Autoridade Nacional de Proteção de Dados (ANPD), acessando https://www.gov.br/anpd/pt-br/canais_atendimento/fale-conosco.

14. Definições

Para os fins desta **Política** aplicam-se as seguintes definições:

- ☐ **Acesso:** direito que o Titular tem de requerer e obter do Controlador informações sobre seus Dados Pessoais tratados;
- ☐ **Agente de Tratamento:** Controlador ou Operador;
- ☐ **Anonimização:** utilização de meios técnicos, razoáveis e disponíveis no momento do Tratamento, por meio dos quais um Dado Pessoal perde a possibilidade de associação, direta ou indireta, a um indivíduo;
- ☐ **ANPD:** Autoridade Nacional de Proteção de Dados;
- ☐ **Armazenamento:** conservação de Dados Pessoais por um Controlador enquanto durar o Tratamento ou por um período exigido;
- ☐ **Avaliação de Interesse Legítimo, Legitimate Interest Assessment ou LIA:** análise que quem trata Dados Pessoais faz para saber se pode aplicar a Base Legal do Interesse Legítimo a um Tratamento;
- ☐ **Averiguação de Conformidade:** análise do grau de aderência à LGPD e à **Política** de qualquer um que mantenha um Contrato ou acordo comercial com a FLUMAR, exceto um Colaborador ou uma Pessoa Relacionada;
- ☐ **Base Legal:** qualquer uma das hipóteses em que o Tratamento de Dados Pessoais é permitido pela LGPD;
- ☐ **Cliente:** cada Cliente da FLUMAR;
- ☐ **Colaborador:** qualquer indivíduo, exceto uma Pessoa Relacionada, que mantenha um contrato de emprego ou de trabalho com a FLUMAR, inclusive administradores, diretores, executivos, investidores, sócios, consultores, assessores, auditores, clientes, parceiros, ocupantes de cargos de gestão ou confiança, empregados, contratados, terceirizados, *trainees*, estagiários, fornecedores e prestadores;
- ☐ **Compartilhamento:** comunicação, difusão, transferência internacional, interconexão de Dados Pessoais ou tratamento compartilhado de bancos de Dados Pessoais entre entidades privadas;
- ☐ **Conformidade:** prática que, por um programa estruturado, visa a que a organização e suas atividades estejam alinhadas com a legislação e com as políticas internas;
- ☐ **Consentimento:** manifestação livre, informada e inequívoca pela qual o Titular concorda com o Tratamento de seus Dados Pessoais para uma Finalidade;
- ☐ **Consultoria Legal:** conjunto de especialistas legais que assessoram a FLUMAR em questões relacionadas à LGPD e a Dados Pessoais e seu Tratamento;

- ☐ *Contrato*: qualquer instrumento jurídico utilizado para expressar a vontade das partes em torno de um negócio; compreende também outros instrumentos de natureza similar, como acordos, termos, ajustes, ordens comerciais e similares;
- ☐ *Controlador*: pessoa natural ou jurídica a quem compete tomar as decisões sobre o Tratamento de Dados Pessoais;
- ☐ *Controle Centralizado*: exigência da LGPD que determina ao Controlador manter um registro consolidado dos Dados que trata e dos Tratamentos que realiza;
- ☐ *Dado Pessoal*: elemento, registro ou referência que identifica ou permite identificar uma pessoa física; *Dado Pessoal Comum*: elemento, registro ou referência geralmente comum à maior parte das pessoas, como nome, endereço, CPF, passaporte, filiação, profissão, *email*, telefone, local de trabalho, naturalidade, CNH, idade, nacionalidade e similares; *Dado Pessoal Sensível*: elemento, registro ou referência sobre origem racial ou
- ☐ étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referente à saúde ou à vida sexual, à genética ou à biometria; *Destinação*: eliminação ou restituição ao Titular dos Dados tratados; *Documentação*: conjunto de evidências materiais (registros, controles, etc.) dos
- ☐ Dados Pessoais tratados e dos Tratamentos a eles aplicados, inclusive quanto à
- ☐ Finalidade, Base Legal e Conformidade à LGPD; *DPO ou Data Protection Officer*: o Encarregado de Dados; *Eliminação*: exclusão de um Dado, ou de um conjunto deles, armazenado em banco de Dados, independentemente do procedimento empregado;
- ☐ *Empresa ou Organização*: a FLUMAR;
- ☐ *Encarregado de Dados*: pessoa nomeada pelo Controlador de Dados Pessoais para atuar como canal entre ele próprio, o Titular dos Dados e a Autoridade Nacional de
- ☐ Proteção de Dados; *Finalidade*: objetivo ou propósito para o qual os Dados Pessoais
- ☐ são tratados;
GDPR ou General Data Protection Regulation: Regulamento 2016/679, em vigor no âmbito da União Europeia, que disciplina e regulamenta o Tratamento e a proteção
- ☐ de Dados Pessoais; *Governança*: sistema de princípios, diretrizes, normas e
- ☐ mecanismos, alinhado às boas práticas de gestão e às normas éticas, que as instituições devem implementar e monitorar para auxiliar a tomada de decisões seguras e responsáveis e para
- ☐ administrar as relações com os *stakeholders* e a sociedade; *Incidente de Segurança*: qualquer evento adverso confirmado que implique violação da segurança de Dados Pessoais – acesso ou divulgação não autorizada, acidental ou ilícita, com destruição, perda, alteração, vazamento, ou tratamento inadequado ou ilícito – e que possa
- ☐ ocasionar risco ou dano relevante ao Titular;
Informação: qualquer conjunto organizado de Dados (Pessoais ou não) com sentido próprio, conteúdo específico e destinação prática;
- Interesse Legítimo*: uma das Bases Legais permitidas pela LGPD para o Tratamento
- ☐ de Dados Pessoais, considerada a mais flexível, mas cuja aplicação só cabe se existe uma justificativa convincente para o Tratamento, se o impacto dele é
- ☐ mínimo sobre a privacidade do Titular e se o Titular, em condições normais, não discordaria do Tratamento de seus Dados;

- ☐ *LGPD*: Lei Geral de Proteção de Dados (Lei nº 13.709/18);
 - ☐ *Operador*: pessoa que faz Tratamento de Dados Pessoais sob ordens ou instruções do Controlador;
 - ☐ *Pessoa Relacionada*: qualquer indivíduo, exceto Colaboradores, cujos Dados Pessoais são tratados porque interagem com a FLUMAR, atuam para ela ou em nome dela, ou que com ela mantenham contrato ou acordo comercial;
 - ☐ *Política*: esta **Política**;
 - ☐ *Portabilidade*: direito que o Titular tem de levar seus Dados Pessoais para Tratamento por um Controlador diferente;
 - ☐ *Propósito Negocial*: qualquer objetivo relacionado à FLUMAR e às suas atividades, como ações administrativas, de pessoal, financeiras, comerciais, de produtos ou serviços, cumprimento de políticas de negócios, *marketing* de negócios, evolução de serviços e outros eventos gerenciais ou operacionais;
 - ☐ *Reclamação*: manifestação formal, endereçada por um Titular à ANPD, com dúvidas, denúncias ou questionamentos sobre o Tratamento de seus Dados por um Controlador ou Operador;
 - ☐ *Regulador*: a Autoridade Nacional de Proteção de Dados (para matérias e assuntos de Dados Pessoais);
 - ☐ *Retenção*: conservação de Dados Pessoais por um período;
 - ☐ *Titular*: indivíduo a quem os Dados Pessoais pertencem;
 - ☐ *Tratamento*: qualquer operação com Dados Pessoais, como coleta, avaliação, produção, utilização, recepção, classificação, eliminação, reprodução, transmissão, acesso, distribuição, controle, processamento, arquivamento, armazenamento, modificação, comunicação, transferência, difusão ou extração;
 - ☐ *Tratamento Automatizado de Dados*: espécie de Tratamento em que um sistema, programa ou tecnologia – incluindo sistemas algorítmicos ou de inteligência artificial – coleta, armazena ou decide com base em Dados Pessoais, sem que haja intervenção humana direta durante esse processo;
 - ☐ *Verificação de Conformidade*: análise do grau de aderência de um Colaborador ou Pessoa Relacionada à LGPD e a esta **Política**;
 - ☐ *Violação*: infração ou descumprimento desta **Política** e (ou) da legislação de proteção de Dados Pessoais.
-