# GUIA DE BOAS PRÁTICAS PARA PROTEÇÃO DE DADOS PESSOAIS

FORÇA AÉREA BRASILEIRA

*Asas que protegem o País*

# SOBRE ESTE GUIA

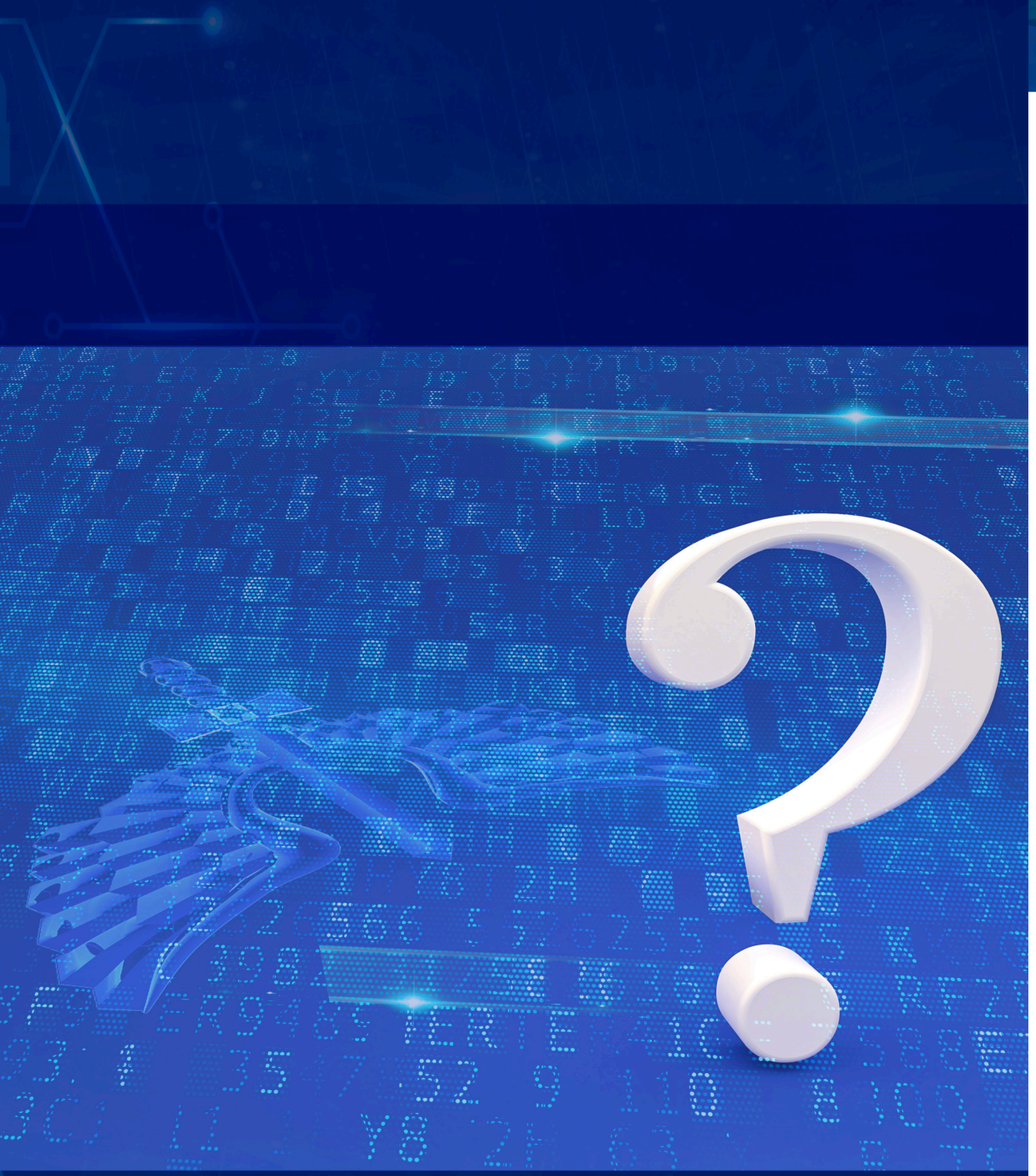
Este guia foi desenvolvido com o objetivo de disseminar as orientações deste Gabinete em relação à lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), bem como alinhar as práticas de seu efetivo à cultura de privacidade e proteção de dados pessoais implantada na Organização.



# A LGPD NÃO VEIO PARA TE DAR MAIS TRABALHO!

A LGPD trouxe profundas mudanças na forma de tratamento dos dados pessoais por empresas, órgãos públicos e pessoas físicas que utilizam tal tratamento para fins econômicos. Isso não significa que essas instituições não possam mais utilizar os dados pessoais, mas se trata de utilizar esses dados de forma responsável, resguardando direitos, garantias e liberdades fundamentais dos seus titulares. Ou seja, a LGPD disciplinou o assunto de forma a haver vantagem para ambos os lados: instituições e titulares de dados. Quando há uma coerência na coleta de dados, há uma confiabilidade maior por parte do titular depositada naquela instituição.

Já imaginou se no processo de consulta para concessão de uma medalha os dados de punição de um militar vazassem para todo o efetivo? E se uma Ata de Inspeção de Saúde de militar ficasse disponível na pasta de acesso comum a todos da Organização? É para evitar situações como essas que a LGPD determinou a adequação de todos os processos que tratem dados pessoais às suas diretrizes.







# MAS... O QUE SÃO DADOS PESSOAIS?

A LGPD conceitua "dados pessoais" como qualquer informação relacionada a uma pessoa física **identificada ou identificável**. Ou seja, podem ser desde um CPF ou RG, um endereço de IP ou e-mail até um posto/graduação ou histórico militar, desde que tais dados possam identificar uma pessoa por meio de quaisquer relações diretas ou indiretas com outras informações. Como exemplo podemos citar o dado "posto de Major-Brigadeiro" com o dado "lotado no GABAER". Tais informações isoladas não significam nada, porém, quando relacionadas, são capazes de identificar o único militar da FAB que é um Major-Brigadeiro servindo no GABAER.

A lei também traz o conceito de dados sensíveis, que são informações com alto potencial de causar problemas discriminatórios ou de cerceamento de direitos dos titulares, tais como: origem étnica, filiação a sindicatos, opinião política, convicção religiosa, dado referente à saúde ou vida sexual, dado genético ou biométrico. Tais dados têm tratamento diferenciado na lei e possuem restrições quanto a sua manipulação.



# OS DIREITOS DOS TITULARES DE DADOS PESSOAIS

O respeito à privacidade e à inviolabilidade da intimidade, da honra e imagem dos titulares são preceitos fundamentais inseridos na realização do tratamento realizado, porque entendemos ser o titular de dados pessoa digna, com direitos a exercer e com liberdade para, a qualquer tempo, questionar o tratamento de seus dados.

É vedada a utilização dos dados por parte do efetivo para finalidades distintas da apontada para realização do tratamento de dados. Também é vedada a utilização dos dados de titulares para fins pessoais ou diversos do especificado, ou seja, que não competentes à Organização.


# QUAIS PRINCÍPIOS DEVEMOS SEGUIR NO TRATAMENTO DE DADOS PESSOAIS?

A LGPD elenca princípios que as instituições devem obrigatoriamente observar no tratamento de dados pessoais. Portanto, além de **agir com boa fé**, todos do efetivo da Organização devem:

• Garantir a qualidade dos dados pessoais dos titulares, prezando pela exatidão, clareza e relevância daqueles;

• Coletar os dados, de forma limitada ao mínimo necessário, para realização das finalidades;

• Realizar o tratamento dos dados com propósitos legítimos, específicos, explícitos e informados, sem a possibilidade de desvirtuar a finalidade do tratamento de dados, que deve, indispensavelmente, ser adequada e informada ao titular;

• Utilizar medidas técnicas e administrativas que podem proteger os dados pessoais de acessos não autorizados;

• Garantir, sendo cooperativo com a equipe, que os titulares de dados tenham acessos de forma facilitada sobre o tratamento realizado e a integralidade de seus dados;

• Ser transparente com o titular de dados, com os colegas e com os responsáveis, dando informações claras e facilmente acessíveis, observadas as regras de sigilo da Organização;

• Evitar, sob qualquer hipótese, agir de forma discriminatória, ilícita ou abusiva; e

• Adotar medidas para prevenir a ocorrência de danos em virtude do tratamento de dados, inseridas na atuação do efetivo, que serão expostas a seguir.



# E QUAIS PRÁTICAS DEVEMOS ADOTAR NO DIA A DIA PARA GARANTIR A PROTEÇÃO DOS DADOS PESSOAIS?

Esta Organização e todos do seu efetivo devem considerar de alta relevância a segurança dos dados, para isso, adotar medidas técnicas e administrativas que garantam proteção ao dado pessoal tratado é de suma importância.

Assim, ao utilizar as medidas preventivas abaixo elencadas e inseri-las na rotina da Organização, seremos capazes de garantir maior proteção aos documentos que contêm dados pessoais.

**Com relação aos telefones funcionais:**

• Lembre-se que o aparelho é da Organização e não seu. Evite usá-lo para fins particulares, baixar aplicativos pessoais e salvar fotos particulares no rolo da câmera do aparelho; e

• Se receber SMS solicitando dados sobre o trabalho, não responda antes de ser autorizado.

**Com relação ao uso de computadores e sistemas organizacionais:**

• A senha de acesso aos sistemas internos da Organização e à rede de computadores deve ser forte, o que significa senha com letra maiúscula, letra minúscula, número e símbolo;

• A senha deve ser trocada periodicamente e, de preferência, a cada três meses;

• Não compartilhe sua senha;

• Não utilize sequências nas senhas, como "1234", "5678", "abcd". Também não utilize "senha" ou "semsenha";

• Tenha cuidados com o computador. Caso levante para tomar água ou ir ao banheiro, bloqueie a tela, para que aqueles que não são do efetivo do setor, não tenham acesso a documentos e informações;

• Não faça downloads de softwares sem conhecimento do Setor de Informática ou acesse sites suspeitos de serem maliciosos; e

• Procure salvar os arquivos sempre na rede de computadores da Organização, evitando salvá-los no HD do computador.



**Com relação ao uso de contas de e-mail:**

• A senha de acesso deve ser forte, o que significa senha com letra maiúscula, letra minúscula, número e símbolo;

• Não compartilhe sua senha;

• Não utilize sequências nas senhas, como "1234", "5678", "abcd". Também não utilize "senha" ou "semsenha";

• Não compartilhe códigos de recuperação de senha ou códigos de acesso;

• Não abra o e-mail corporativo em computador que não seja o próprio de trabalho, a não ser que esteja em ***home office***; e

• Se recebeu um e-mail que acredita ser SPAM, pedimos que informe ao Setor de Informática e não o responda.

**Com relação ao *home office*:**

• Utilize apenas o e-mail corporativo para tratar de assuntos do setor de trabalho;

• Configure o seu roteador, inserindo uma senha forte e protegendo-o contra o risco de invasão desse dispositivo. Se precisar, solicite o auxílio do Setor de Informática;

• Tenha um bom antivírus instalado na sua máquina e sempre realize o escaneamento do computador antes de utilizá-lo;

• Sempre utilize a VPN fornecida por Unidade do Comando da Aeronáutica para realizar os trabalhos remotos. Ela cria uma espécie de proteção entre o computador pessoal e o servidor da Organização, bloqueando possíveis invasores. Assim, é possível acessar documentos desse servidor com segurança;

• Tenha critério ao armazenar documentos e dados da Organização na "nuvem". O ***backup*** de documentos e informações classificadas ou sigilosas na nuvem é proibido, conforme Norma Complementar nº 14/IN01/DSIC/SCS/GSIPR, de 13 de março de 2018.

• A mesma Norma citada anteriormente determina que os serviços computacionais em nuvens só poderão ser utilizados por Órgãos da Administração Federal se definidos em instrumento contratual ou similar. Ou seja,  é vedado o tratamento de informações da Organização em ambientes de computação em nuvens sem a autorização da Alta Administração da Organização.

• Evite o envio de documentos e informações de trabalho via aplicativos de mensagens como *Telegram e Whatsapp*.




**Descarte de papéis e mídias:**

• O descarte de documentos físicos (papéis, cds, dvds, pendrives, disquetes, filmes, cartões de memória e Hds) que contenham dados pessoais deve ser feito seguindo as orientações da SPADAER, e efetivado por meio da utilização de trituradores que possuam nível de segurança a partir do nível 3 da Norma DIN 66399, deixando não identificáveis quaisquer dados.

• O descarte de rascunhos, listas e relações também devem ocorrer por meio de trituradores no padrão acima descrito.

• Estude a possibilidade de adotar a utilização de aplicativos que eliminam definitivamente os arquivos de computadores e celulares, tais como o ***Eraser*** e o ***Android Data Eraser***.

• Promova uma gestão documental de forma a observar fielmente a temporalidade da guarda de documentos. Manter sob sua posse dados pessoais além do previsto atenta às determinações da LGPD.

**Com relação à atuação no Setor de Trabalho:**

• Não fale com pessoas de fora do Setor sobre os titulares dos dados tratados, nem sobre os processos e procedimentos.

• Não fale com pessoas de fora do Setor de Trabalho sobre os dados dos militares e servidores do efetivo da Organização.

• Ao receber uma solicitação, seja de fornecedor, de um superior de outra OM ou de alguém do efetivo da Organização, informe-a imediatamente aos responsáveis, que a irão responder prontamente.

• Evite manter papéis ou documentos que contenham dados pessoais em cima da mesa quando você não estiver no Setor. Prefira guardá-los em armários ou gavetas com trancas e acesso restrito às chaves.

• Não permita que pessoas estranhas ao Setor tenham acesso a documentos e dados pessoais que estejam sendo tratados por você. Restrinja ao máximo o acesso aos dados pessoais àquelas pessoas indispensáveis ao seu tratamento.

• Evite a impressão de documentos que contenham dados pessoais. Essa prática reduz drasticamente a chance de ocorrer um incidente de dados.

• Invista na criação de rotinas e procedimentos de armazenamento de documentos em meio físico, designando responsáveis, critérios e normas de manuseio, determinando quais podem ser acessados por todos e quais terão acesso restrito.

# TEM DÚVIDAS SOBRE OS PASSOS PARA ADEQUAÇÕES DOS PROCESSOS DO SEU SETOR À LGPD?

As novas determinações contidas na LGPD demandam a realização de adequações nos processos existentes na Organização. Também é preciso que os novos processos que porventura surjam na OM estejam em conformidade com a referida lei.

**Observe abaixo os principais passos para adequação dos processos à LGPD:**

• Realizar o mapeamento de todos os processos que envolvam tratamento de dados pessoais, descrevendo o processo de coleta, todos os tipos de tratamento realizado, o armazenamento, compartilhamento, bem como verificando se há tratamento de dados pessoais sensíveis.

• Definir as bases legais mais apropriadas para o tratamento de dados, conforme a finalidade específica.

analisar se há discrepâncias entre as obrigações e princípios definidos na LGPD e as práticas dos processos da Organização, definindo quais estratégias adotar para a adequação.

• Definir os responsáveis por cada ação dentro dos processos.

• Implementar ferramentas que permitam aos titulares de dados pessoais exercerem seus direitos garantidos pela LGPD.

• Elaborar, revisar, adaptar e aditar contratos que envolvam tratamento e/ou compartilhamento de dados pessoais nas relações com fornecedores.

• Controlar e monitorar se a implementação das adequações está acontecendo conforme o planejamento.

• Manter a cultura de privacidade e proteção de dados pessoais no setor de trabalho, inclusive nos novos processos criados, de forma a manter a aderência da Organização à LGPD.

**SURGIU DÚVIDAS SOBRE ESTE GUIA?**

A LGPD prevê a existência da figura do Encarregado pelo Tratamento de Dados Pessoais em todas as instituições. Essa pessoa é o elo entre a Organização e a Autoridade Nacional de Proteção de Dados, bem como entre a Organização e os titulares de dados pessoais.

A DCA 16-6/2020 – Governança da Proteção de Dados no COMAer, editada pelo EMAER, nomeou essa figura como **Encarregado Setorial** e, normalmente, essa função recai na figura do Chefe da Assessoria de Governança (AsGov) ou Assessoria de Planejamento, Orçamento e Gestão (APOG) da Organização.

Caso você seja contatado por algum titular de dado pessoal que queira exercer algum direito previsto na LGPD, o encaminhe para o Encarregado Setorial da OM. Assim você contribui para que a Organização não corra riscos em relação ao cumprimento da legislação, e também estará prestando um serviço de qualidade aos militares e servidores da FAB que necessitam do apoio da sua OM.

É importante que você saiba quem é o Encarregado Setorial da sua Organização. É a ele que você deverá encaminhar possíveis dúvidas ou sugestões sobre o conteúdo deste Guia!

**FORÇA AÉREA BRASILEIRA**

*Asas que protegem o País*