

**MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA**



GOVERNANÇA

DCA 16-6

**GOVERNANÇA DA PROTEÇÃO DE DADOS
PESSOAIS DO COMANDO DA AERONÁUTICA**

2021

**MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
ESTADO-MAIOR DA AERONÁUTICA**



GOVERNANÇA

DCA 16-6

**GOVERNANÇA DA PROTEÇÃO DE DADOS
PESSOAIS DO COMANDO DA AERONÁUTICA**

2021



MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
GABINETE DO COMANDANTE DA AERONÁUTICA

PORTARIA GABAER Nº 197/GC3, DE 15 DE DEZEMBRO DE 2021.

Aprova a Diretriz que dispõe sobre a Governança da Proteção de Dados Pessoais do Comando da Aeronáutica.

O COMANDANTE DA AERONÁUTICA, no uso das atribuições que lhe confere o inciso I e XIV do Art. 23 da Estrutura Regimental do Comando da Aeronáutica, aprovada pelo Decreto nº 6.834, de 30 de abril de 2009, e considerando o que consta no Processo nº 67050.014803/2021-60, procedente do Estado-Maior da Aeronáutica, resolve:

Art. 1º Aprovar a reedição da DCA 16-6 “Governança da Proteção de Dados Pessoais do Comando da Aeronáutica”, que com esta baixa.

Art. 2º Art. 3º Revoga-se a Portaria nº 899/GC3, de 28 de agosto de 2020, publicada no Boletim do Comando da Aeronáutica nº 156, de 31 de agosto de 2020.

Art. 3º Esta Portaria entra em vigor 3 de janeiro de 2022.

Ten Brig Ar CARLOS DE ALMEIDA BAPTISTA JUNIOR
Comandante da Aeronáutica

(Publicado no BCA nº232, de 20 de dezembro de 2021)

SUMÁRIO

1 DISPOSIÇÕES PRELIMINARES	9
1.1 <u>FINALIDADE</u>	9
1.2 <u>CONCEITUAÇÕES</u>	9
1.3 <u>ÂMBITO.....</u>	9
2 PRESSUPOSTOS NORMATIVOS	10
2.1 <u>LEI 13.709/2018</u>	10
2.2 <u>DECRETO 10.046/2019</u>	10
2.3 <u>DCA 16-1/2019 - GOVERNANÇA NO COMAER</u>	10
3 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS	11
3.1 <u>CONSIDERAÇÕES BASILARES.....</u>	12
3.2 <u>O CICLO DE VIDA DOS DADOS PESSOAIS</u>	13
3.3 <u>TÉRMINO DO TRATAMENTO</u>	14
3.4 <u>NÃO APLICAÇÃO DA LGPD.....</u>	14
3.5 <u>REGISTRO DAS OPERAÇÕES DE TRATAMENTO DE DADOS PESSOAIS (RTD)</u>	15
3.6 <u>RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)</u>	15
3.7 <u>BOAS PRÁTICAS EM SEGURANÇA DAS INFORMAÇÕES</u>	16
4 ESTRUTURA DE GOVERNANÇA DE PROTEÇÃO DE DADOS PESSOAIS DO COMAER	20
4.1 <u>RESPONSABILIDADES CONFORME À LGPD</u>	20
4.2 <u>CONTROLADOR DO COMAER - CMTAER</u>	21
4.3 <u>CONSELHO DIRETIVO DE TECNOLOGIA DA INFORMAÇÃO - CONTI.....</u>	21
4.4 <u>ENCARREGADO DO COMAER - EMAER (6SC)</u>	21
4.5 <u>CONTROLADOR SETORIAL - ODGS.....</u>	22
4.6 <u>ENCARREGADO DE COORDENAÇÃO - REPRESENTANTE ODGSA</u>	22
4.7 <u>CONTROLADOR ORGÂNICO - CMT de OM.....</u>	22
4.8 <u>CONTROLADOR TÉCNICO - DTI.....</u>	22
4.9 <u>OUVIDORIA - CECOMSAER.....</u>	22
4.10 <u>OPERADORES</u>	23
4.11 <u>COMITÊ EXECUTIVO DE TECNOLOGIA DA INFORMAÇÃO - COMEX-TI....</u>	23
5 DISPOSIÇÕES GERAIS	24
5.1 <u>ASPECTOS GERAIS A SEREM CONSIDERADOS</u>	24
6 DISPOSIÇÕES ESPECÍFICAS	25
6.1 <u>ESTADO-MAIOR DA AERONÁUTICA - EMAER</u>	25
6.2 <u>TODOS OS ODGSA</u>	25
6.3 <u>COMANDO GERAL DE APOIO - COMGAP</u>	26
6.4 <u>COMANDO GERAL DE PESSOAL - COMGEP</u>	27
6.5 <u>CENTRO DE COMUNICAÇÃO SOCIAL DA AERONÁUTICA - CECOMSAER..</u>	27
7 DISPOSIÇÕES FINAIS	29
REFERÊNCIAS	30

PREFÁCIO

A Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018) foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo, por intermédio da regulação do tratamento de dados pessoais, em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado, o qual abarca um amplo conjunto de operações efetuadas em meios manuais ou digitais.

Nesse contexto, a Governança no compartilhamento de dados na Administração Pública Federal, autárquica e fundacional também segue as diretrizes estabelecidas no Decreto nº 10.046, de 9 de outubro de 2019, e precisa ser compreendida à luz das restrições legais, dos requisitos de segurança da informação e comunicações e do disposto pela LGPD.

Outrossim, com fundamento nesses dois diplomas legais, o Comitê Central de Governança de Dados redigiu o Guia de Boas Práticas para orientar a implementação dos princípios e regras da LGPD na Administração Pública Federal.

Sendo assim, o Estado-Maior da Aeronáutica (EMAER), por meio do estudo desses três documentos, buscou consignar no presente documento importantes diretrizes de Governança de Proteção de Dados Pessoais para todo o COMAER, a fim de que a instituição como um todo busque promover um aperfeiçoamento de seus processos e sistemas, com o escopo de adequá-los aos interesses da sociedade representados pelos diplomas legais citados e pelo Ordenamento Jurídico brasileiro como um todo.

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

A finalidade precípua da presente publicação de Governança de Proteção de Dados Pessoais do Comando da Aeronáutica é orientar o aperfeiçoamento dos processos que envolvam o tratamento de dados pessoais à luz da Lei Geral de Proteção de Dados Pessoais (LGPD) e das demais legislações em vigor relacionadas ao tema.

1.2 CONCEITUAÇÕES

Os termos e expressões empregados neste documento constam no Glossário da Aeronáutica (MCA 10-4), no Glossário das Forças Armadas (MD35-G-01) e no Artigo 5º da LGPD.

1.3 ÂMBITO

Esta diretriz aplica-se a todas as Organizações do Comando da Aeronáutica.

2 PRESSUPOSTOS NORMATIVOS

A seguir se descrevem as principais normas que fundamentam os preceitos consignados na presente Diretriz.

2.1 LEI 13.709/2018

A Lei 13.709, de 14 de agosto de 2018, a qual foi alterada pela Lei 13.853, de 8 de julho de 2019, e que é conhecida por Lei Geral de Proteção de Dados Pessoais (LGPD), foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. Essa Lei versa sobre o tratamento de dados pessoais, **dispostos em meio físico ou digital**, feito por pessoa física ou jurídica de direito público ou privado e engloba um amplo conjunto de operações efetuadas sobre o ciclo de vida desses dados pessoais.

2.2 DECRETO 10.046/2019

O Poder Executivo promulgou o Decreto 10.046, de 9 de outubro de 2019, a fim de dispor sobre a Governança no compartilhamento de dados no âmbito da Administração Pública Federal e instituir o Comitê Central de Governança de Dados, com fundamento na LGPD, além de também instituir o Cadastro Base do Cidadão, com base no Art. 11 da Lei nº 13.444, de 11 de maio de 2017.

2.3 DCA 16-1/2019 GOVERNANÇA NO COMAER

O Estado-Maior da Aeronáutica consolidou na DCA 16-1 os princípios, a organização e a dinâmica de funcionamento da Governança no Comando da Aeronáutica. Esse documento é essencial uma vez que a própria DCA 16-6 descreve que a estrutura de Governança de Proteção de Dados Pessoais do COMAER deve se inter-relacionar com a estrutura de Governança do COMAER, prevista na DCA 16-1.

3 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

3.1 CONSIDERAÇÕES BASILARES

3.1.1 A LGPD define, logo em seu Artigo 1º, o escopo de suas disposições, qual seja, o tratamento de dados pessoais feito em meios físicos ou digitais, por pessoas físicas e jurídicas de direito público ou privado. As regras dispostas na lei têm por objetivo a proteção da privacidade, da liberdade e do livre desenvolvimento da personalidade das pessoas naturais.

3.1.2 Em função disso, o tratamento de dados pessoais se revela como ponto central da Lei e merece maior dedicação em compreendê-lo. Antes mesmo de definir e exemplificar o que é tratamento, salienta-se o conceito de dado pessoal, qual seja: “informação relacionada a pessoa natural identificada ou identificável” (Art. 5º, LGPD).

3.1.3 Diferentemente da Lei de Acesso à Informação (Lei nº 12.527/2011), os direitos e salvaguardas sobre dados pessoais da LGPD incidem sobre todos os tipos de dados pessoais, observadas as legislações existentes, inclusive os regimes existentes de transparência e acesso à informação.

3.1.4 Sendo assim, como é descrito nesta DCA, a tutela da lei se estende não mais apenas aos dados pessoais sensíveis ou diretamente relacionados aos direitos de personalidade, mas, em maior ou menor medida, a todos os dados pessoais.

3.1.5 O Decreto nº 10.046/2019 buscou agrupar esses dados pessoais em categorias o que torna mais racional a gestão de informações pelos órgãos e entidades públicas. Desta forma, à taxonomia de dados pessoais já existente, soma-se o conteúdo da tabela a seguir:

Categorias de dados pessoais	Descrição
Atributos biográficos	Dados de pessoa natural relativos aos fatos da sua vida, tais como nome civil ou social, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, grupo familiar, endereço e vínculos empregatícios. Tais atributos poderão ser considerados como dados pessoais sensíveis, se o seu conteúdo se referir à convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político.
Atributos biométricos	Características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, conforme Art. 2º, inciso II do Decreto 10.046/2019, os quais, por definição legal, constituem-se em dados pessoais sensíveis.
Atributos genéticos	Características hereditárias da pessoa natural, obtidas pela análise de ácidos nucleicos ou por outras análises científicas, os quais, por definição legal, constituem-se em dados pessoais sensíveis.
Dados cadastrais	Informações identificadoras perante os cadastros de órgãos públicos, tais como atributos biográficos, em conjunto com dados como números de cadastro tais como CPF, CNPJ, NIS, PIS, PASEP e Título de Eleitor.

Tabela 1 – Categorias de Dados Pessoais.

3.1.6 O dado pessoal é coletado para atender a uma finalidade específica e pode, por exemplo, ser eliminado a pedido do titular dos dados (LGPD, Art. 18, IV), para o cumprimento de uma sanção aplicada pela Autoridade Nacional de Proteção de Dados (ANPD)(LGPD, Art. 52, VI) ou ao término de seu tratamento (LGPD, Art. 16), compreendendo um ciclo que se inicia com a coleta e que determina a “vida” (existência) do dado pessoal, durante um determinado período, de acordo com certos critérios de eliminação.

3.1.7 É fundamental destacar que a LGPD considera como tratamento toda operação realizada com dados pessoais, como “coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração” (Art. 5º, inciso X da LGPD).

3.1.8 Esse rol de atividades apresentados na Lei é meramente exemplificativo, ou seja, quaisquer outras atividades que envolverem dados pessoais também serão consideradas como tratamentos, mesmo que esteja fora dessa lista.

3.1.9 Sendo assim, toda e qualquer operação com o dado pessoal deve ter ao menos uma hipótese legal autorizativa e deve adotar as medidas necessárias para melhor proteção do conteúdo pessoal em operação, com especial zelo relacionado aos princípios que a LGPD destaca em seu Artigo 6º.

3.1.10 O primeiro desses princípios é a finalidade, ou seja, o tratamento tem que ser realizado para fins legítimos, específicos, explícitos e informados ao titular do dado. É importante também que o tratamento seja adequado e necessário, bem como que seja de livre acesso aos titulares a consulta sobre a forma, duração e integralidade de seus dados pessoais. Além disso, é preciso que os dados pessoais mantenham a qualidade, com exatidão, clareza e precisão, sendo relevante também a transparência no tratamento e a utilização de medidas de segurança e prevenção contra danos aos titulares. É vedada, ainda, a utilização do tratamento para fins discriminatórios. Por fim, o agente de tratamento é responsável e deve prestar contas do cumprimento das normas pertinentes na realização das operações com dados pessoais.

3.2 O CICLO DE VIDA DOS DADOS PESSOAIS

3.2.1 Para implementar o correto tratamento dos dados pessoais e as medidas correlatas, o órgão precisa conhecer esses dados que gerencia e quais processos, projetos, serviços e ativos perpassam o ciclo de vida do tratamento dos dados pessoais.

3.2.2 Entende-se por ciclo de vida do tratamento dos dados pessoais todas as ações realizadas desde a coleta do dado até sua eliminação ou descarte. Este ciclo é composto por cinco grandes fases, onde cada uma das atividades de tratamento de dados está inserida.



Figura 1 – Ciclo de vida do tratamento de dados pessoais.

3.2.3 A primeira fase do ciclo de vida do tratamento dos dados se dá através da **coleta**, onde os dados são produzidos ou recepcionados independente do meio utilizado (documento em papel, documento eletrônico, sistema de informação etc.).

3.2.4 Uma vez coletados os dados entram na segunda etapa do ciclo de vida que é a **retenção**. Nesta fase são realizadas o arquivamento ou armazenamento de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, banco de dados, arquivo de aço etc.).

3.2.5 Estes dados também passam pelo **processamento**, que é representado por qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação e extração e modificação de dados pessoais retidos pelo controlador.

3.2.6 O **compartilhamento**, por sua vez, envolve qualquer operação de transmissão, distribuição, comunicação, transferência, difusão e uso compartilhado de dados pessoais.

3.2.7 Por fim, a **eliminação** é qualquer operação que visa excluir um dado ou conjunto de dados pessoais armazenados em banco de dados, em virtude do tratamento da LGPD. Quando se tratar da eliminação de documentos arquivísticos, devem ser levadas em consideração as recomendações constantes no item 3.3 desta DCA.

Dados Pessoais	
Fase do ciclo de tratamento	Operações de tratamento – LGPD, Art. 5º, X
Coleta	Coleta, produção, recepção
Retenção	Arquivamento e armazenamento
Processamento	Classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação
Compartilhamento	Transmissão, distribuição, comunicação, transferência e difusão
Eliminação	Eliminação

Tabela 2 – Relacionamento das fases do ciclo de vida X operações sobre dados pessoais.

3.3 TÉRMINO DO TRATAMENTO

3.3.1 Uma vez que o dado pessoal coletado alcançou a finalidade para o qual foi coletado este não deve mais permanecer sob tratamento da organização. Desta forma cada dado pessoal coletado para uma determinada finalidade terá um marco que representará o término de seu tratamento.

3.3.2 Nos termos da LGPD, o término do tratamento de dados pessoais ocorre em quatro hipóteses:

- a) exaurimento da finalidade para os quais os dados foram coletados ou quando estes deixam de ser necessários ou pertinentes para o alcance desta finalidade;
- b) fim do período de tratamento;
- c) revogação do consentimento a pedido do titular, resguardado o interesse público; e
- d) determinação da Autoridade Nacional em face de violação do disposto na LGPD.

3.3.3 Para se definir quando uma informação não é mais necessária, as organizações devem se basear em normativos e regulamentos que estabeleçam os prazos de guarda e destinação final que cada documento deverá seguir. Tal definição permite que a organização somente tenha sob sua posse os dados pessoais que realmente são necessários para a execução de suas

atividades. Importante salientar que os prazos de guarda e destinação final aplicam-se tanto à documentos físicos quanto digitais.

3.3.4 Ressalta-se que o COMAER atualmente utiliza-se do código de classificação e tabela de temporalidade e destinação de documentos relativos às atividades-meio do Poder Executivo Federal e o código de classificação e tabela de temporalidade e destinação de documentos de arquivo relativos às atividades-fim do Ministério da Defesa como referências para determinar o prazo de guarda e armazenamento das informações, bem como sua destinação final.

3.3.5 No âmbito da Administração Pública, é importante que os preceitos da LGPD sejam harmonizados com a legislação de arquivos, em especial com o que preceitua a Lei nº 8.159/1991, e suas regulamentações. Isso porque, desse ponto de vista, os dados pessoais coletados pelo poder público passam a constituir o que se denomina arquivo público (Art. 7º), e, sendo assim, a sua eliminação deverá obedecer, também, a classificação arquivística pertinente, de acordo com o valor arquivístico de cada documento.

3.3.6 Além disso, ainda sobre a Lei nº 8.159/1991, na eliminação de documentos produzidos por instituições públicas e de caráter público é realizada mediante autorização da instituição arquivística pública, na sua específica esfera de competência (Art. 9º). Sendo assim, mesmo que exaurida a finalidade precípua da coleta (primeira hipótese levantada), o dado pessoal poderá compor documento de valor permanente, por sua natureza histórica, probatória ou informativa, o qual tem natureza inalienável e imprescritível (Art. 10).

3.4 NÃO APLICAÇÃO DA LGPD

3.4.1 No tocante ao Tratamento de Dados Pessoais para Segurança do Estado e Defesa Nacional (Segurança Pública como um todo) a LGPD prevê em seu Artigo 4º, inciso III, que a referida Lei não se aplica aos tratamentos de dados pessoais realizados **exclusivamente** para defesa nacional, segurança pública, segurança do Estado e atividades de investigação criminal.

3.4.2 Mesmo a LGPD não se aplicando aos dados pessoais tratados exclusivamente para os fins apresentados acima, é importante que os responsáveis por estas atividades de tratamento de dados não se omitam em relação aos princípios e diretrizes apresentados na Lei, vez que, segundo o § 3º do Artigo 4º, a Autoridade Nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas e deverá solicitar aos responsáveis os Relatórios de Impacto à Proteção de Dados Pessoais.

3.5 REGISTRO DAS OPERAÇÕES DE TRATAMENTO DE DADOS PESSOAIS (RTD)

3.5.1 A Lei Geral de Proteção de Dados Pessoais, em seu Artigo 37, discorre sobre a necessidade do controlador e do operador manterem registro das operações de tratamento de dados pessoais que realizarem. Para que isso seja possível, é fundamental saber como esses dados são tratados desde a sua coleta até o final da sua utilização. Buscando representar este entendimento obtido, a utilização do Registro das Operações de Tratamento de Dados Pessoais (ou inventário de dados pessoais) é uma forma clara e objetiva de retratar essa dinâmica. Esse documento mostra que tipo de informação tramitará durante a execução do processo, de onde os dados virão e onde serão armazenados e/ou compartilhados.

3.5.2 O EMAER e a Diretoria de Tecnologia da Informação (DTI) realizaram, em conjunto com algumas organizações militares, o mapeamento de suas principais operações de

tratamento de dados. Importante ressaltar que esses são documentos vivos e dinâmicos e que precisam ser periodicamente avaliados, conforme a ocorrência de mudanças significativas na estrutura desses processos.

3.5.3 Destaca-se ainda que é de suma importância que os Registros das Operações de Tratamento de Dados Pessoais (RTD), bem como os novos processos a serem mapeados e registrados sejam atualizados, conforme a publicação de novas diretrizes e recomendações e estejam em conformidade com toda a legislação vigente sobre proteção de dados.

3.6 RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

3.6.1 Uma vez conhecendo suas operações de tratamento de dados pessoais o COMAER deve verificar e demonstrar conformidade quanto a esse tratamento realizado. Esta verificação pode se dar através da elaboração do Relatório de Impacto à Proteção dos Dados Pessoais (RIPD), documento elaborado pelo controlador, que tem como objetivo identificar e descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação aos riscos identificados (Art. 5º, inciso XVII).

3.6.2 São elencadas algumas hipóteses a serem consideradas para que se proceda com a elaboração deste Relatório, tais como:

- a) quando houver tratamento de dado pessoal sensível (Art. 5º, inciso II e Art. 38 da LGPD);
- b) quando houver tratamento de dados pessoais de crianças e adolescentes (Art. 14 da LGPD);
- c) quando o tratamento de dados pessoais que possam resultar em algum tipo de dano patrimonial, moral, aos titulares desses dados (Art. 42 da LGPD);
- d) quando o tratamento de dados pessoais tiver como base legal o legítimo interesse do controlador (Art. 10, § 3º da LGPD);
- e) quando houver alterações nas leis e regulamentos aplicáveis à privacidade, política, normas internas ou operação do sistema de informações; e
- f) quando houver reformas administrativas que impliquem em nova estrutura organizacional.

3.6.3 Destaca-se que a ANPD deverá regulamentar posteriormente, de forma mais detalhada, os procedimentos relacionados ao RIPD. Desta forma recomenda-se o acompanhamento das regulamentações que serão expedidas pela ANPD, a fim de que o COMAER mantenha atualizado o modelo de RIPD já estabelecido, utilizado e se prepare para eventuais solicitações.

3.6.4 É importante que a Força Aérea Brasileira esteja atenta às solicitações de RIPD por parte da ANPD, dado que a ausência ou atraso na elaboração deste documento pode ensejar razão suficiente para a aplicação de uma sanção administrativa ou de processos judiciais em desfavor do COMAER. Para isso, é essencial que toda movimentação de dados pessoais esteja fundamentada nas devidas hipóteses legais.

3.7 BOAS PRÁTICAS EM SEGURANÇA DAS INFORMAÇÕES

3.7.1 Além dos diversos normativos elaborados pelo COMAER com orientações sobre os mais detalhados e específicos temas de segurança da informação e privacidade, é fundamental que também sejam considerados outras instruções apresentadas pelos órgãos competentes, no intuito de trazer novos entendimentos sobre esses assuntos e orientar como a Força pode implementar tais dinâmicas.

3.7.2 A Secretaria do Governo Digital do Ministério da Economia, por exemplo, tem preparado um conjunto de ações para fomentar a cultura de proteção de dados e apoiar a evolução da maturidade necessária às adequações da lei nos órgãos do Governo Federal.

3.7.3 Nessa jornada para a adequação à LGPD, são sugeridos métodos, materializados em forma de guias operacionais para consulta e que tem sido constantemente atualizado para atender os novos entendimentos sobre o tema.

3.7.4 Desta forma é recomendável que os agentes de tratamento considerem sempre tais instruções, a fim de aumentarem seu nível de maturidade acerca desses temas, bem como se manterem alinhados às estratégias dos demais órgãos da Administração Pública Federal.

3.7.5 PADRÕES E CONTROLES DE SEGURANÇA CIBERNÉTICA

3.7.5.1 Para que o COMAER alcance um alto grau de maturidade quanto à gestão de seus riscos de segurança cibernética e proteção de dados pessoais é importante que sejam considerados alguns modelos ou frameworks, que apresentam um conjunto de técnicas, ferramentas ou conceitos pré-definidos que auxiliam na implementação das melhores práticas para o gerenciamento de seus riscos.

3.7.5.2 A seguir se descrevem iniciativas e documentos técnicos relacionados com esses aspectos e que podem servir como importante fonte de consulta e orientação para o COMAER, naquilo que couber, dentre eles:

- a) **ePING**: conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da Tecnologia de Informação e Comunicação (TIC) na interoperabilidade de serviços de Governo Eletrônico;
- b) **ABNT NBR ISO/IEC 27001:2013**: norma que especifica os requisitos para se estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão da Segurança da Informação (SGSI), bem como os requisitos para avaliação e tratamento de riscos de segurança da informação, sempre com o foco nas necessidades da organização;
- c) **ABNT NBR ISO/IEC 27002:2013**: norma que estipula as melhores práticas para apoiar a implantação do SGSI, com diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização;
- d) **ABNT NBR ISO 31000:2018**: norma que referencia os fundamentos prolatados pela DCA 16-2 “Gestão de Riscos no COMAER”, constituindo-se num documento com recomendações relevantes para o gerenciamento de riscos das organizações, podendo ser personalizado para qualquer contexto;

- e) **ABNT NBR ISO/IEC 27701:2019:** norma que especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação (SGPI) no contexto da organização; e
- f) **Normativos do Gabinete de Segurança Institucional da Presidência da República (GSI/ PR):** normativos elaborados pelo GSI/PR e de cumprimento obrigatório pelos órgãos e entidades da Administração Pública Federal, direta e indireta e que tem por objetivo auxiliar no aumento da maturidade da Segurança da Informação e elevação dos níveis de proteção dos dados.

3.7.6 PRIVACIDADE DESDE A CONCEPÇÃO (*PRIVACY BY DESIGN*)

3.7.6.1 A Lei Geral de Proteção de Dados Pessoais dispõe, expressamente, em seu Artigo 46, que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger esses dados presentes em sistemas, bancos de dados ou em documentos físicos, independente da fase do ciclo de vida do tratamento dos dados pessoais.

3.7.6.2 Portanto, todos os agentes de tratamento que participarem de quaisquer fases do ciclo de vida do tratamento de dados pessoais serão responsáveis por assegurar medidas técnicas de segurança necessárias para a proteção de dados pessoais.

3.7.6.3 Complementarmente, o Artigo 46 da LGPD, em seu parágrafo 2º, dispõe sobre a necessidade de que as medidas de segurança, técnicas e administrativas deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. Esta definição faz referência direta ao conceito de Privacidade desde a Concepção (do inglês *Privacy by Design*).

3.7.6.4 Tal conceito consiste na proteção dos dados pessoais em todo o ciclo de vida do processo, sendo amparado por princípios fundamentais que serão apresentados, enfatizando a importância da proteção desde a criação do processo. São esses os princípios:

Princípio	Descrição
Proativo não reativo / preventivo não reativo	A Privacidade desde a Concepção é caracterizada por medidas proativas em vez de reativas. Isso quer dizer que há uma antecipação dos eventos invasivos de privacidade antes da sua existência real. Portanto, não se espera que de fato ocorra um evento danoso para tomar as medidas de segurança necessárias, mas visa evitá-los.
Proteção de dados como configuração padrão	A proteção de dados como configuração padrão consiste na proteção máxima dos dados pessoais por mecanismos de segurança suficientes, incluindo sistemas de TI ou práticas de negócios, capazes de garantir maior grau de privacidade. O objetivo deste princípio é evitar que o titular de dados precise realizar ações para garantir a sua privacidade, que já estará assegurada pelos mecanismos da organização.
Privacidade incorporada ao projeto	A proteção de dados deverá abranger desde o <i>design</i> à arquitetura dos sistemas de Tecnologia de Informação e práticas de negócios, não devendo ser um complemento posterior ou adicional. O objetivo deste princípio é garantir que a privacidade seja essencial para a funcionalidade do processo como um todo, sendo parte do sistema sem atingir a sua funcionalidade.

Funcionalidade total	A proteção de dados desde a concepção visa contemplar todos os interesses dos setores, de forma que exista uma complementariedade, pretendendo satisfazer todos os objetivos da organização e não somente os de privacidade.
Segurança de ponta a ponta	A Privacidade desde a Concepção consiste na proteção à privacidade antes mesmo que seja coletada a primeira informação pessoal, amparando o ciclo de tratamento de dados no processo, projeto, sistema ou serviço, aplicando medidas de segurança do início ao fim. Este princípio visa garantir que o ciclo de vida dos dados pessoais siga de forma segura, onde serão coletados com a devida proteção e, no final do processo, destruídos com segurança, permitindo um gerenciamento deste ciclo. Neste mesmo sentido, dispõe a LGPD (Artigo 6º, inciso VII) ao apresentar os princípios essenciais para o tratamento de dados pessoais, inclusive a segurança.
Visibilidade e Transparência	A Privacidade desde a Concepção visa garantir a transparência durante todo o ciclo de vida dos dados pessoais, isso significa dizer que, independentemente de prática ou tecnologia envolvida, o tratamento de dados deverá ocorrer somente de acordo com as premissas e objetivo declarado. Nesse sentido, visibilidade e transparência são essenciais para uma organização que deseja ser reconhecida pelo respeito à privacidade. Para atingir este objetivo, é recomendável que seja realizada uma avaliação, observando os princípios previstos no Artigo 6º da Lei Geral de Proteção de Dados Pessoais.
Respeito à privacidade do usuário	A Privacidade desde a Concepção leva em consideração a experiência e privacidade do titular de dados pessoais. Nesse sentido, exige-se que os interesses dos titulares dos dados pessoais estejam em primeiro lugar, oferecendo todas as medidas de gerenciamento destes dados, sendo uma forma mais eficiente contra abusos e uso indevido por parte das instituições. Por isso, a lei determina, expressamente, alguns aspectos que deverão ser observados quando for necessário o tratamento de dados pessoais. Os Artigos 7º e 11 da LGPD apresentam as hipóteses legais que darão embasamento ao tratamento de dados pessoais.

Tabela 3 – Princípios do Privacy by Design (Cavoukian, Ann. 2013).

3.7.7 PRIVACIDADE POR PADRÃO (PRIVACY BY DEFAULT)

3.7.7.1 Os agentes de tratamento deverão adotar medidas suficientes de segurança, técnicas e administrativas para proteger, por padrão, os dados pessoais processados para atingir a sua finalidade definida previamente.

3.7.7.2 Portanto, conforme o princípio da necessidade disposto no artigo 6º, II da LGPD, somente deverão ser processados os dados pessoais necessários para cada finalidade específica do processamento, levando-se em consideração a quantidade de dados pessoais coletados, a extensão de seu processamento, o período de armazenamento e a acessibilidade.

3.7.7.3 A Privacidade por Padrão exige o cumprimento de boas práticas, como:

- a) **Finalidade:** deverá ser informado ao titular de dados, antes mesmo de quaisquer processamentos, a finalidade para que estes foram coletados,

retidos, usados e/ou divulgados. Esta comunicação deverá ser clara, específica e de forma explícita;

- b) **Limitação da Coleta:** a coleta deve ser limitada aos fins específicos apresentados ao titular e legalmente reconhecidos;
- c) **Minimização dos dados:** deverá ser coletado apenas os dados realmente necessários para atingir a finalidade informada ao titular, observando obter o mínimo de informações pessoais; e
- d) **Limitação de uso, retenção e divulgação:** Os dados somente poderão ser retidos de acordo com a finalidade e pelo tempo apresentado ao titular de dados. Portanto, o uso, retenção e divulgação somente ocorrerão diante das finalidades identificadas pelo titular de dados, para os quais a lei permite ou por ele foram consentidas.

4 ESTRUTURA DE GOVERNANÇA DE PROTEÇÃO DE DADOS PESSOAIS DO COMAER

4.1 RESPONSABILIDADES CONFORME À LGPD

4.1.1 A Lei Geral de Proteção de Dados Pessoais trouxe, a partir de seu Artigo 5º, alguns papéis, a definição de suas atividades e responsabilidades atinentes ao tratamento dos dados pessoais, além de apresentar seus deveres jurídicos. O entendimento adequado de tais atribuições é fundamental para sua efetiva execução. São os atores envolvidos, basicamente: o titular de dados pessoais, os agentes de tratamento, divididos em controlador e operador, e o encarregado de dados.

4.1.2 O **titular de dados pessoais** é definido como “pessoa natural a quem se referem os dados pessoais que são objeto de tratamento” (Art. 5º, V). Por intermédio da LGPD, resta claro que os dados pertencem ao titular e que as instituições são somente usuárias desses dados, mediante autorização pelo consentimento ou outra base legal legítima e pelo tempo estritamente necessário para contemplar a finalidade pretendida.

4.1.3 O **controlador**, é definido pela Lei como a “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” (Art. 5º, VI). Na prática, é a figura que determina como deve ser realizado o tratamento dos dados pessoais. É também o responsável pela indicação do encarregado de dados (Art. 41).

4.1.4 O **operador**, por sua vez, é compreendido como “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador” (Art. 5º, VII), ou seja, é aquele que realizará o tratamento conforme definido pelo controlador. Cabe ao controlador verificar se as instruções foram seguidas pelo operador.

4.1.5 Por fim, a LGPD apresenta a figura do **encarregado**. Este é visto como peça-chave para a organização, vez que será responsável e atuará como canal de comunicação entre o controlador, os titulares dos dados e a ANPD, inclusive para fins de realização de consulta prévia, reforçando seu papel expressamente consignado na Lei. Dessa forma, como determina o Art. 41, §1º, da referida Lei, a identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

4.1.6 Considerando a magnitude e complexidade de se estabelecer um Programa de Governança em Privacidade em todo o COMAER e a autonomia que muitas vezes as instituições têm entre si, entendeu-se como necessário que estes atores apresentados na LGPD fossem expandidos de maneira que, dentro de cada estrutura, existissem agentes de tratamento responsáveis pela efetiva implementação deste programa.

4.1.7 A seguir é apresentada a estrutura de Governança de Proteção de Dados Pessoais do COMAER, a qual deve se inter-relacionar com a estrutura de Governança do COMAER como um todo, prevista na DCA 16-1 “Governança no COMAER”.

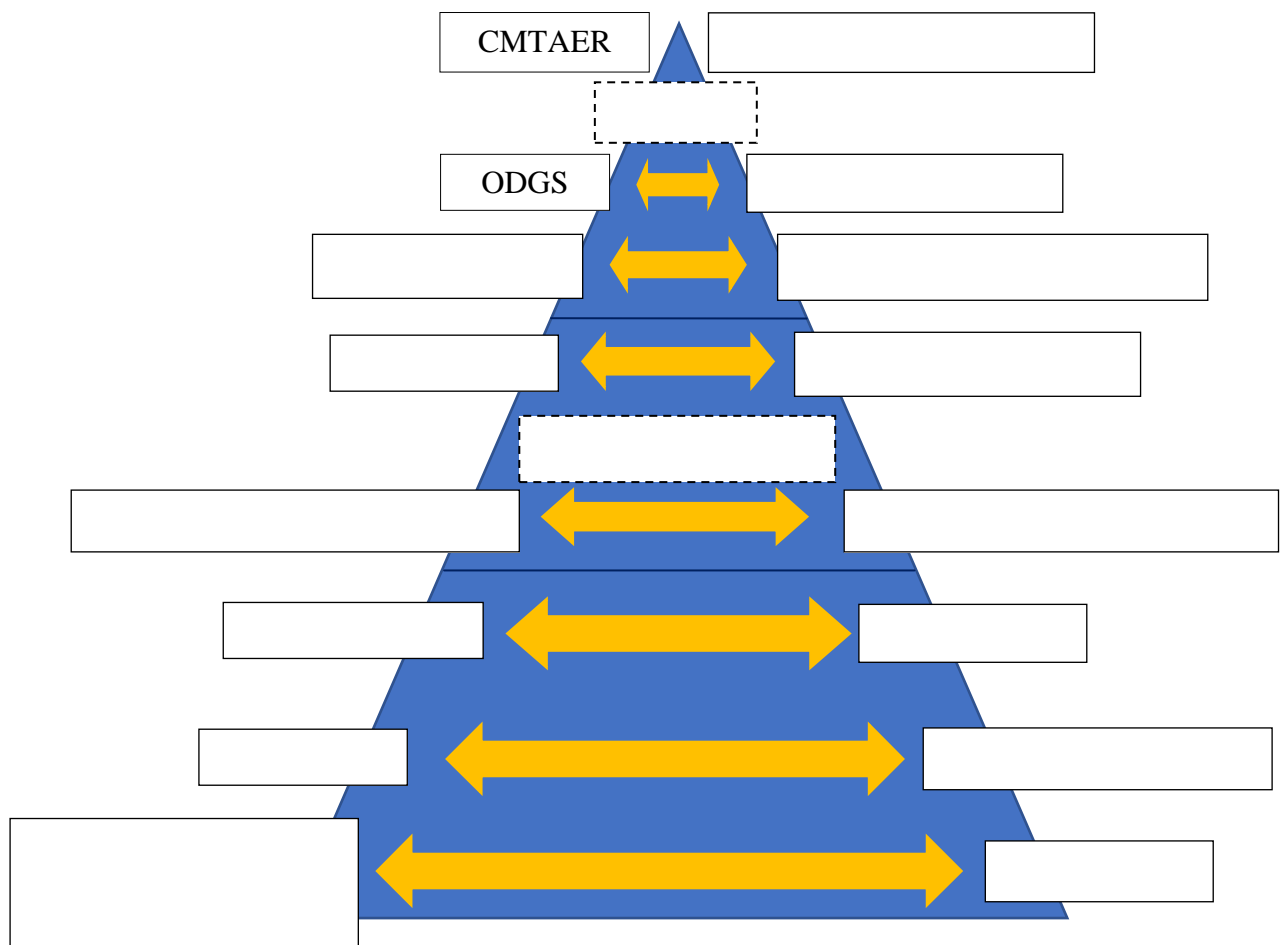


Figura 2 – Estrutura de Governança de Proteção de dados pessoais do COMAER.

4.2 CONTROLADOR DO COMAER - CMTAER

Em observância à LGPD e conforme destacado no item 4.1.3, o Comandante da Aeronáutica, na condição de dirigente máximo da instituição, é considerado o Controlador do COMAER, sendo o responsável por toda a Governança Digital e de Privacidade de Dados Pessoais da Força. No entanto, para apoiá-lo nessa função, compartilhando com ele essa responsabilidade, foi criada uma estrutura de Governança, conforme a figura 2.

4.3 CONSELHO DIRETIVO DE TECNOLOGIA DA INFORMAÇÃO - CONTI

Conforme o Art. 2º, §1º, IV do Decreto 10.332, de 28 de abril de 2020, o Comitê de Governança Digital dos órgãos da Administração Pública Federal passará a contar com a participação do Encarregado do Tratamento de Dados Pessoais do órgão. No COMAER, essa estrutura é denominada CONTI (Conselho Diretivo de Tecnologia da Informação), que conta ainda com a avaliação preliminar dos assuntos, por meio do Comitê Executivo de Tecnologia da Informação (COMEX-TI), realizando apreciação técnica das pautas que serão deliberadas no CONTI.

4.4 ENCARREGADO DO COMAER - EMAER (6SC)

O EMAER, aqui representado pelo Chefe da 6ª Subchefia (6SC) do Estado-Maior da Aeronáutica, é o responsável por exercer a função de Encarregado do COMAER,

tendo como principal atribuição servir como um canal de comunicação qualificado entre a estrutura de Governança de Proteção de Dados da organização, a ANPD, os titulares, bem como com os demais órgãos de controle externo da Administração Pública Federal.

4.5 CONTROLADOR SETORIAL - ODGS

Cada Órgão de Direção Geral e Setorial (ODGS) que participa do CONTI, aqui representado pelos Chefes/Diretores/Secretário/Comandantes, deve exercer uma responsabilidade específica e solidária pelo tratamento de dados afeto aos processos ou sistemas sob a gerência de seus Órgãos, sendo, pois, considerados, no COMAER, como Controladores Setoriais. Embora tal figura não esteja explicitamente prevista na LGPD, ela converge para o desiderato promovido pela referida lei, de uma estrutura de Governança de Proteção de Dados Pessoais efetiva e presente em todo o organograma institucional.

4.6 ENCARREGADO DE COORDENAÇÃO - REPRESENTANTE ODGSA

Atuarão como Encarregado de Coordenação os Elos de Coordenação de TI, de todos os Órgãos de Direção Geral, Setorial e Assistência Direta (ODGSA), que compõem o Comitê Executivo de Tecnologia da Informação (COMEX-TI). Assim, o Encarregado de Coordenação também terá um papel importante na orientação dos militares de sua unidade, além das OM Subordinadas, a respeito das práticas a serem tomadas em relação à proteção de dados pessoais, bem como executar as demais atribuições determinadas pelo respectivo Controlador Setorial ou Controlador Orgânico, além do pronto atendimento às solicitações que forem demandadas pelo Encarregado do COMAER.

4.7 CONTROLADOR ORGÂNICO - CMT de OM

Para todas as demais Organizações Militares (OM), aqui representada pelo seu Comandante, este será considerado o Controlador Orgânico, pois diante da complexidade e das dimensões da estrutura organizacional da FAB, além da autonomia que cada OM tem de decidir como deverá ser realizado o tratamento dos dados pessoais, esse fato não o impede de, quando aplicável, realizar esse tratamento seguindo a orientação dos Controladores Setoriais para aquelas atividades sob sua responsabilidade, bem como indicarem seus próprios “encarregados” ou “elos de coordenação” para auxiliarem os respectivos Encarregados de Coordenação.

4.8 CONTROLADOR TÉCNICO - DTI

Uma vez que a Diretoria de Tecnologia da Informação da Aeronáutica, órgão central do Sistema de Tecnologia da Informação, tem o papel fundamental na tomada de decisão de como serão realizados e de quais meios de Tecnologia da Informação serão empregados nos tratamentos de dados no âmbito de seus sistemas de informação e infraestrutura tecnológica, a DTI atua intensamente no ciclo de vida do tratamento de dados pessoais em sua fase digital, justificando a designação do Diretor como Controlador Técnico do COMAER.

4.9 OUVIDORIA - CECOMSAER

O Centro de Comunicação Social da Aeronáutica (CECOMSAER) deve desempenhar a função de Canal de Comunicação da Governança de Dados do COMAER conjuntamente com as suas atribuições afetas à Lei de Acesso à Informação e ao Decreto nº 9.492, de 5 de setembro de 2018. Em consonância a isso, o CECOMSAER deve se valer da

estrutura do Sistema de Comunicação Social da Aeronáutica (SISCOMSAE) para distribuir as demandas recebidas da sociedade que estão relacionadas à LGPD aos Encarregados do COMAER e de Coordenação.

4.10 OPERADORES

Conforme descrito no item 4.1.4, os Operadores são empresas que realizam tratamento de dados em nome do COMAER, aos quais se deve especial atenção quanto as cláusulas contratuais sobre o respectivo tratamento e aos riscos envolvidos nessa relação à luz da privacidade de dados pessoais.

4.11 COMITÊ EXECUTIVO DE TECNOLOGIA DA INFORMAÇÃO - COMEX-TI

Em consonância com o avançado processo evolutivo do Conselho Diretivo de TI, com o oportuno suporte das pautas avaliadas no COMEX-TI, as ações de Governança de Proteção de Dados Pessoais do COMAER encontrarão na ICA 7-47 um normativo de referência para as atribuições a serem realizadas pelos Encarregados de Coordenação sobre a LGPD, que atuarão de forma integrada, com consciência situacional ampla e sem prejuízo às demandas relativas à segurança da informação e a governança de TI no Sistema de Tecnologia da Informação (STI).

5 DISPOSIÇÕES GERAIS

A seguir são descritas as orientações gerais para todo o COMAER, acerca dos principais aspectos da LGPD.

5.1 ASPECTOS GERAIS A SEREM CONSIDERADOS

5.1.1 É importante destacar que todo tratamento de dados pessoais que necessite ser realizado deverá seguir as diretrizes da LGPD de forma justa e transparente, além de ser desenvolvido para uma finalidade específica, explícita e legítima.

5.1.2 Além disso, devem ser observados os princípios e recomendações da Privacidade desde a Concepção e Por Padrão, apresentados nos itens 3.7.6 e 3.7.7 desta DCA, não só no âmbito dos sistemas da informação, mas em todas as atividades e processos a serem executados.

5.1.3 Quaisquer alterações que se façam necessárias nos processos de negócio e nos sistemas de informação deverão ser alvo de uma avaliação de impacto à privacidade para, previamente, entender o impacto de tais alterações no Programa de Governança em Privacidade do COMAER.

5.1.4 Também é reforçada a necessidade de que todos os responsáveis por processos de negócio que realizem o tratamento de dados pessoais façam o registro dessas atividades de maneira padronizada e as mantenham atualizadas, a fim de permitir um mapeamento de como cada processo de negócio realiza esse tratamento e com qual fundamentação legal. Os Encarregados, tanto no nível COMAER quanto no nível dos ODGSA, serão pontos focais quanto a orientações sobre as práticas a serem tomadas para garantir a segurança e proteção dos dados pessoais.

5.1.5 Frise-se que é de competência do Encarregado de Coordenação a avaliação de impacto à privacidade nos processos de negócio da Força, bem como o registro das atividades e operações de tratamento que envolvam dados pessoais. Sendo da competência do Controlador Técnico essa mesma avaliação de impacto nos sistemas de informação do COMAER.

5.1.6 No que se refere as hipóteses de consentimento, no COMAER a maioria dos processos de tratamento de dados internos não requerem consentimento. Portanto, há que se analisar cada caso concreto, para se verificar a incidência da obrigatoriedade do consentimento do titular de dados, especialmente nos processos que envolvam informações de pessoas que não tenham vínculo institucional com a Organização.

5.1.7 Além disso, é importante levar em consideração que, para o caso de dados pessoais de crianças e adolescentes, sempre será necessário o consentimento dos seus responsáveis.

5.1.8 Por fim, os Órgãos do COMAER devem analisar em que medida as regras e princípios consignados nos dispositivos da LGPD aplicam-se a cada processo organizacional sob a sua responsabilidade, porquanto a lei somente alcança a sua plenitude, quando aplicada a cada caso concreto. Neste contexto, é importante que todas as Organizações se utilizem do método preconizado pela DCA 16-5 “Gestão por Processos no COMAER”, para realizarem o mapeamento de seus processos, analisando em que medida a atividade administrativa ou operacional se vale do tratamento de dados pessoais e em qual hipótese da lei este tratamento se enquadra.

6 DISPOSIÇÕES ESPECÍFICAS

A seguir são descritas as orientações específicas para os ODGSA, a fim de que se promovam as adaptações que necessariamente devem ser realizadas na sua estrutura e nos seus processos organizacionais, a fim de implementar os requisitos da LGPD.

6.1 ESTADO-MAIOR DA AERONÁUTICA - EMAER

Observar o que se segue:

- a) executar todas as atividades esperadas do Encarregado, conforme orientações do Art. 41 da LGPD;
- b) avaliar, monitorar e direcionar as atividades relacionadas ao Programa de Governança da Privacidade de Dados Pessoais, bem como ao processo de adequação do COMAER à LGPD;
- c) assessorar o Comandante da Aeronáutica nas decisões afetas ao integral cumprimento da LGPD;
- d) receber reclamações e solicitações dos titulares dos dados pessoais, prestando esclarecimentos e adotando providências, com subsídios dos Encarregados de Coordenação, sempre que for o caso; e
- e) representar a instituição, no tocante à privacidade e proteção de dados, perante a sociedade como um todo, bem como junto à ANPD e aos demais órgãos de controle externo da Administração Pública Federal.

6.2 TODOS OS ODGSA

A seguir, são descritas as atribuições comuns a todos os ODGSA e OM subordinadas:

- a) nomear o Encarregado de Coordenação, para que ele exerça a função descrita no item 4.6 desta DCA;
- b) inventariar todos os processos de negócios que realizam tratamento de dados pessoais sob sua responsabilidade através do Registro das Operações de Tratamento de Dados (RTD), como orientado no item 3.5 desta DCA;
- c) identificar todos os processos de negócio que realizam tratamento de dados pessoais sob sua responsabilidade, que tenham como finalidade exclusiva a segurança pública, defesa nacional, segurança do Estado, para o caso de ser necessária a elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD) para estes processos;
- d) elaborar, quando determinado pela ANPD ou pelo Encarregado do COMAER, Relatório de Impacto à Proteção de Dados Pessoais (RIPD), referente a suas operações de tratamento de dados;
- e) manter contratos e normativos internos que orientem quanto ao tratamento de dados pessoais adequados aos princípios e requisitos da LGPD;
- f) manter atualizados todos os Registros de Operação de Tratamento de Dados (RTD), o Plano de Ação, o Plano de Respostas e o Relatório de Impacto à Proteção de Dados Pessoais (quando aplicável), bem como todas as medidas técnicas e administrativas implementadas para proteger os dados pessoais de

acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, ou qualquer forma de tratamento inadequado ou ilícito, sempre em condições de serem disponibilizados ao Encarregado do COMAER, para o atendimento tempestivo, sempre que necessário e solicitado por este;

- g) comunicar imediatamente ao Encarregado do COMAER a ocorrência de qualquer incidente de segurança que possa acarretar risco ou dano relevante aos titulares, mencionando a descrição da natureza dos dados pessoais afetados, as informações sobre os titulares envolvidos, a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, os riscos relacionados ao incidente, as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo, conforme o procedimento de notificação de incidentes de segurança da Força;
- h) garantir que o tratamento dos dados pessoais em seus processos de negócios se dê somente pelo tempo estritamente necessário para alcançar sua finalidade, seguindo as orientações das tabelas de temporalidade do COMAER, não só nos meios físicos, mas também nos meios digitais;
- i) por meio do Encarregado de Coordenação, responder às demandas dos titulares de dados pessoais que apresentarem solicitações referentes aos tratamentos desses dados sob a responsabilidade do ODGSA, e
- j) assumir a responsabilidade na observância aos princípios de Privacidade desde a Concepção e Por Padrão, apresentados nos itens 3.7.6 e 3.7.7 desta DCA, que também pertence aos donos das regras de negócio. E ratificando o disposto no item 5.1.2, todos são responsáveis pela Segurança da Informação e devem trabalhar em conjunto com o órgão central do STI, para garantir a confiabilidade nos sistemas de informação.

6.3 COMANDO-GERAL DE APOIO - COMGAP

Além das atribuições comuns descritas no item 6.2, observar o que se segue, por meio da atuação da DTI:

- a) subsidiar os demais ODGSA na adequação das bases de dados e sistemas de TI que estejam relacionados com alguma fase do ciclo de tratamento de dados pessoais;
- b) coordenar a estruturação dos sistemas de TI utilizados para o tratamento de dados pessoais de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de Governança e aos princípios gerais previstos na LGPD, às demais normas regulamentares e, oportunamente, às disposições da ANPD;
- c) executar as etapas de contenção, erradicação, recuperação e elaboração de lições aprendidas quando da ocorrência de um incidente de segurança da informação no âmbito dos sistemas da informação e bases de dados do COMAER, que possa acarretar risco ou dano relevante aos titulares de dados;
- d) realizar avaliações periódicas de segurança nos sistemas de informação da FAB, para garantir que não apresentem brechas ou vulnerabilidades que impactem na segurança e na proteção dos dados pessoais;

- e) implementar avisos de privacidade nos sistemas de informação ou portais da FAB que disponibilizem mecanismos de coleta de informações pessoais;
- f) garantir que os princípios de Privacidade desde a Concepção e Por Padrão, apresentados nos itens 3.7.6 e 3.7.7 desta DCA, sejam considerados em todo o ciclo de desenvolvimento dos sistemas da informação do COMAER; e
- g) seguir os guias e recomendações para o desenvolvimento e manutenção de segurança nos sistemas de informação propostas pela Secretaria do Governo Federal e pelo Gabinete de Segurança Institucional da Presidência da República.

6.4 COMANDO-GERAL DO PESSOAL - COMGEP

Além das atribuições comuns descritas no item 6.2, observar o que se segue:

- a) com o apoio da DTI e dos elos do Sistema de Tecnologia da Informação (STI) no que couber, realizar, principalmente por meio da atuação da DIRAP, as adequações em processos, base de dados, sistemas e normas, relativas ao tratamento dos dados pessoais do efetivo da ativa, da reserva, bem como dependentes e pensionistas, levando em conta as especificidades do tratamento de dados pessoais de crianças e de adolescentes;
- b) com o apoio da DTI e dos elos do STI no que couber, realizar, principalmente por meio da atuação da DIRENS, as adequações em processos, base de dados, sistemas e normas, relativas ao tratamento do Sistema de Ensino da Aeronáutica (SISTENS), levando em conta as especificidades do tratamento de dados pessoais de crianças e de adolescentes;
- c) com o apoio da DTI e dos elos do STI no que couber, realizar, principalmente por meio da atuação da DIRSA, as adequações em processos, base de dados, sistemas e normas, relativas ao tratamento do Sistema de Saúde da Aeronáutica (SISAU), levando em conta as especificidades do tratamento de dados pessoais de crianças e de adolescentes; e
- d) realizar as adequações em processos no que se refere a temporalidade no tratamento dos dados. É essencial o fortalecimento da conscientização referente aos dispostos no Art. 15 e no Art. 16 da LGPD, que tratam das hipóteses para o término do tratamento de dados pessoais. Esse trabalho deve alcançar todas as organizações do COMAER, sendo o CENDOC observado como o principal colaborador para o referido processo.

6.5 CENTRO DE COMUNICAÇÃO SOCIAL DA AERONÁUTICA - CECOMSAER

Além das atribuições comuns descritas no item 6.2, observar o que se segue:

- a) estruturar o setor de Lei de Acesso à Informação/Ouvidoria para atuar como canal de comunicação entre a sociedade brasileira e os responsáveis pelo tratamento de dados pessoais no COMAER;
- b) receber reclamações e comunicações de titulares de dados pessoais e dos demais entes da sociedade brasileira, como a ANPD, através dos canais de comunicação oficiais da FAB e encaminhá-las para o Encarregado para que

possam ser respondidas e assegurando o envio das respostas aos demandantes;

- c) manter atualizado no sítio oficial do COMAER, <http://www.fab.mil.br/>, com base no entendimento do Encarregado do COMAER, as informações acerca dos procedimentos e práticas utilizadas pela instituição para o tratamento de dados pessoais, conforme prevê a LGPD; e
- d) estabelecer e executar um programa contínuo de conscientização sobre a segurança da informação, a proteção e a privacidade dos dados pessoais para todo o efetivo do COMAER, com o suporte do EMAER, do COMGEP e da DTI.

7 DISPOSIÇÕES FINAIS

Esta Diretriz deve ser atualizada por iniciativa do Estado-Maior da Aeronáutica, em coordenação com os ODSA, sempre que julgado necessário.

REFERÊNCIAS

ANN CAVOUKIAN. *Privacy by Design. The 7 Foundational Principles*. Disponível em: <<https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>> Acesso em: 24 jul. 2021.

BRASIL. Associação Brasileira de Normas Técnicas. **ABNT NBR ISO 31000:2018** - Gestão de Riscos – Diretrizes. 2018.

_____. Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27002:2013**: Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação - Requisitos. 2013

_____. Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27002:2013**: Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação. 2013.

_____. Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27701:2019** Sistema de Gerenciamento de Informações de Privacidade (PIMS). 2019.

_____. Comando da Aeronáutica. Centro de Documentação da Aeronáutica. “Confecção, Controle e Numeração de Publicações Oficiais do Comando da Aeronáutica”: **NSCA 5-1**. Rio de Janeiro, RJ, 2011.

_____. Comando da Aeronáutica. Diretoria de Tecnologia da Informação. “Regras de funcionamento do COMEX-TI do COMAER”: **ICA 7-47**. São Paulo, SP, 2019.

_____. Comando da Aeronáutica. Estado-Maior da Aeronáutica. “Gestão de Riscos no COMAER”: **DCA 16-2**. Brasília, DF, 2018.

_____. Comando da Aeronáutica. Estado-Maior da Aeronáutica. “Gestão por Processos no COMAER”: **DCA 16-5**. Brasília, DF, 2019.

_____. Comando da Aeronáutica. Estado-Maior da Aeronáutica. “Glossário da Aeronáutica”: **MCA 10-4**. Brasília, DF, 2001.

_____. Comando da Aeronáutica. Estado-Maior da Aeronáutica. “Governança no COMAER”: **DCA 16-1**. Brasília, DF, 2019.

_____. Decreto nº 9.492, de 5 de setembro de 2018. Regulamenta a Lei nº 13.460, de 26 de junho de 2017, que dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública federal, institui o Sistema de Ouvidoria do Poder Executivo federal, e altera o Decreto nº 8.910, de 22 de novembro de 2016, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Transparência, Fiscalização e Controladoria-Geral da União.

_____. Decreto nº 10.046, de 9 de outubro de 2019. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.

_____. Decreto nº 10.332, de 28 de abril de 2020. Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências.

_____. Lei nº 8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências.

_____. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso às informações (Lei de Acesso à Informação - LAI).

_____. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).

_____. Ministério da Defesa. “Código de classificação e tabela de temporalidade e destinação de documentos de arquivo relativos às atividades-fim do Ministério da Defesa”. Brasília, DF, 2013.

_____. Ministério da Justiça. “Código de classificação e tabela de temporalidade e destinação de documentos relativos às atividades-meio do Poder Executivo Federal”. Rio de Janeiro, RJ, 2020.