ESCOLA SUPERIOR DE GUERRA

ESG

DIRETRIZ PARA A PROTEÇÃO DE DADOS PESSOAIS NA ESCOLA SUPERIOR DE GUERRA

ESCOLA SUPERIOR DE GUERRA

ESG

ESCOLA SUPERIOR DE GUERRA

ESG

DIRETRIZ PARA A PROTEÇÃO DE DADOS PESSOAIS NA ESCOLA SUPERIOR DE GUERRA

1ª edição 2025

Comandante

General de Divisão ALEXANDRE OLIVEIRA CANTANHEDE LAGO

Subcomandante

Brigadeiro do Ar IVAN LUCAS KARPISCHIN

Departamento de Estudos

Brigadeiro do Ar (R1) HELIO SEVERINO DA SILVA FILHO

Instituto Therezinha de Castro

Prof. Dr. JACINTHO MAIA NETO

Departamento de Administração

Coronel VINICIUS CORDEIRO RAMIREZ

Centro de Tecnologia da Informação e Comunicação

CF (RM1-T) APARECIDA NUNES DA SILVA

Assessoria Jurídica

2° Tenente MARIO JORGE ROCHA DE SOUZA

Encarregada da Lei Geral de Proteção de Dados

1° Tenente VERÔNICA FERNANDES SOARES

SUMÁRIO

Introdução

A proteção de dados pessoais, um tema de grande relevância, tem recebido cada vez mais atenção e regulamentação em nível mundial. No cenário nacional, a Lei Geral de Proteção de Dados Pessoais (LGPD), promulgada pela Lei nº 13.709, em 14 de agosto de 2018, delimitou sua incidência no artigo 1º, abrangendo o tratamento de dados pessoais, inclusive nos meios digitais, por pessoas naturais ou jurídicas, públicas ou privadas, com o objetivo de proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade.

Reconhecendo a importância dessa legislação, a Escola Superior de Guerra (ESG) instituiu, por meio da Portaria nº 2845, de 5 de junho de 2024, uma comissão para elaborar diretrizes internas de aplicação da LGPD. Esse esforço resultou na "Diretriz para a Proteção de Dados Pessoais", aprovado pela Portaria n° 160, de 14 de maio de 2025, a qual é composta por doze capítulos, que consolidam os principais aspectos da lei, adaptados às particularidades da ESG. Com a publicação da versão 2.0 do Guia Orientativo para Definições dos Agentes de Tratamentos de Dados Pessoais e do Encarregado, em abril de 2022, pela Autoridade Nacional de Proteção de Dados (ANPD), torna- se necessário criar e manter atualizadas as diretrizes para garantir um melhor entendimento das responsabilidades dos agentes de tratamento de dados pessoais.

Capítulo 1 – Disposições Gerais

1.1 Propósito

Dispor sobre o tratamento de dados pessoais na Escola Superior de Guerra (ESG), nos termos da LGPD.

1.2 Aplicabilidade

O disposto na LGPD é aplicável ao tratamento de dados pessoais de pessoa natural realizado na ESG, inclusive por meio digital, exceto quando realizado:

a) por pessoa natural para fins exclusivamente particulares e não econômicos;

b) para fins exclusivamente jornalístico, artísticos ou acadêmicos (este último mediante consentimento);

c) para fins exclusivos de:

- atividades de investigação e repressão de infrações penais;

- defesa nacional;
- segurança do Estado; ou
- segurança pública.

No que se refere à alínea c, a LGPD veda o tratamento dos dados por pessoa de direito privado, exceto em procedimentos sob tutela da ESG, que serão objeto de informe específico à ANPD, observando-se, ainda, que o seu capital seja integralmente constituído pelo poder público.

A ANPD emitirá opiniões técnicas ou recomendações referentes às exceções previstas na alínea c, acima, mencionada, e deverá solicitar a elaboração de relatórios de impacto à proteção de dados pessoais.

1.3 Fundamentos

De acordo com a LGPD, a disciplina da proteção de dados pessoais tem como fundamentos:

a) respeito à privacidade;
b) autodeterminação informativa;
c) liberdade de expressão, de informação, de comunicação e de opinião;
d) inviolabilidade da intimidade, da honra e da imagem;
e) desenvolvimento econômico e tecnológico e inovação;
f) livre iniciativa, livre concorrência e defesa do consumidor; e
g) direitos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania pelas pessoas naturais.

1.4 Princípios de Proteção de Dados Pessoais

As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

a) finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

b) adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

c) necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

d) livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

e) qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

f) transparência: 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, além da proteção às informações consideradas imprescindíveis à segurança da sociedade e do Estado, esta última nos termos do art. 23 da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI);

g) segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

h) prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

i) não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e

j) responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

1.5 Requisitos para o Tratamento de Dados Pessoais

O tratamento de dados pessoais no âmbito da ESG será promovido de forma a atender à finalidade pública, na busca do interesse público. Entende-se como tratamento toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

a) mediante o fornecimento de consentimento pelo titular;

b) cumprimento de obrigação legal ou regulatória pelo controlador da ESG;

c) para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do capítulo IV da LGPD;

d) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

e) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

f) para o exercício regular de direitos em processo judicial, administrativo ou arbitral, este último nos termos da Lei nº 9.307/1996 (Lei de Arbitragem);

g) para a proteção da vida ou da incolumidade física do titular ou de terceiro;

h) para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

i) quando necessário para atender aos interesses legítimos do controlador da ESG ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; e

j) para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Capítulo 2 – Conceitos e Definições

As seguintes definições devem ser consideradas para os fins desta Diretriz:

2.1. Dado: pode ser classificado como:

a) dado pessoal: é a informação relacionada à pessoa natural identificada ou identificável. Também serão considerados aqueles utilizados para a formação do perfil comportamental de determinada pessoa, se identificada;

b) dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à 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;

c) dado anonimizado: dado relativo a titular que não possa ser

identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. O dado anonimizado não é considerado dado pessoal para os fins da LGPD, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido; e

d) dado pseudoanonimizado: dado submetido a tratamento por meio do qual perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador da ESG em ambiente controlado e seguro.

2.2. Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

2.3. Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

2.4. Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

2.5. Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independente do procedimento empregado.

2.6. Agentes de Tratamento de dados:

a) controlador: a LGPD atribuiu aos órgãos públicos obrigações típicas de controlador, indicando que, no setor público, essas obrigações devem ser distribuídas entre as principais unidades administrativas despersonalizadas que integram a pessoa jurídica de direito público e realizam tratamento de dados pessoais. Nesse sentido, a União, como controladora, é a responsável perante a LGPD, mas as atribuições de controlador, por força da desconcentração administrava, são exercidas pelos órgãos públicos que desempenham funções em nome da pessoa jurídica da qual fazem parte. As atividades relativas à adequação da Organização à LGPD são realizadas pelos agentes públicos por meio dos mecanismos próprios de exercício do poder diretivo dos órgãos, bem como por meio da atribuição interna de responsabilidades e competências. Portanto, para condução das atividades da LGPD na ESG foi estabelecida a seguinte atribuição:

I) a ESG exercerá as funções típicas de controlador, subsidiado, no que se refere à dimensão estratégica do assunto, pelo Comitê de Governança Digital da ESG.

b) operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do

controlador da ESG.

2.7. Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

2.8. Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública, estruturada pelo Decreto nº 10.474/2020, responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

2.9. Encarregado do Tratamento de Dados Pessoais: Oficial designado, pelo controlador em Portaria, para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

2.10. Órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

2.11. Unidade Organizacional responsável pelo tratamento de dados pessoais corresponde a todo componente da estrutura organizacional da ESG que realize operação de tratamento de dados pessoais.

2.12. Relatório de impacto à proteção de dados pessoais: documentação do controlador da que contém a descrição dos 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 de risco.

Capítulo 3 – Governança

3.1. O Comitê de Governança Digital da ESG acompanhará, em nível estratégico, as ações relacionadas ao tratamento de dados pessoais, por meio da estrutura de governança estabelecida, competindo-lhe:

I - subsidiar o Comando nos temas afetos à proteção de dados pessoais;

II - aprovar o Programa de Gestão em Privacidade (PGP), bem como suas revisões;

III - orientar e monitorar a implementação do PGP, acompanhando seus indicadores; e

IV - apreciar propostas e sugerir aperfeiçoamentos nas diretrizes, políticas, procedimentos e estruturas relacionados à proteção de dados pessoais em conformidade com as disposições da Lei nº 13.709 de 2018 (LGPD).

3.2. O PGP tem por objetivos aperfeiçoar as operações de tratamento de dados pessoais e promover um ciclo de melhoria contínua para cumprir a legislação e normativos pertinentes, consolidando os requisitos de privacidade e proteção de dados pessoais no âmbito da Escola Superior de Guerra.

3.3. O PGP deverá conter no mínimo:

I - ações que visem elevar o nível de maturidade da proteção de dados pessoais;

II - plano de comunicação que estabeleça os procedimentos internos e as formas de comunicação com os titulares de dados pessoais e com a ANPD; e

III - modelos padronizados de inventário de dados, de relatório de impacto à proteção de dados pessoais e de plano de resposta a incidentes.

3.4. O PGP deverá considerar as prioridades e as peculiaridades da ESG para o cumprimento desta Diretriz.

3.5 Na implementação dos procedimentos para o tratamento de dados pessoais, a unidade organizacional responsável, considerando o volume e a natureza dos dados tratados, deverá adotar, ao menos, as seguintes boas práticas:

I - mapear as atividades de tratamento e realizar o inventário dos dados pessoais tratados, mantendo-o atualizado;

II - elaborar o relatório de impacto à proteção de dados pessoais quando necessário;

III - adotar medidas de transparência aos usuários sobre o tratamento de dados pessoais, por meio do sítio institucional da ESG da internet;

IV - fazer cumprir, no âmbito de suas atribuições e competências, a Política de Segurança da Informação;

V - determinar, no âmbito de suas atribuições e competências, que terceiros contratados estejam em conformidade com a LGPD; e

VI - incentivar a participação em eventos de capacitação, visando estimular a cultura de proteção de dados pessoais.

Capítulo 4 – Mapeamento e Inventário de Dados Pessoais

4.1. A unidade organizacional responsável pelo tratamento de dados pessoais deverá realizar o mapeamento e o inventário dos dados pessoais sob sua custódia.

4.2. O mapeamento de dados pessoais consiste na atividade de identificar os dados pessoais objeto de tratamento e o seu ciclo de vida, bem como seus repositórios e banco de dados.

4.3. O mapeamento de dados pessoais inclui todas as operações de tratamento, a compreender:

I - coleta;

II - retenção;

III - processamento;

IV - compartilhamento;

V - eliminação; e

VI - demais operações em que dados pessoais estejam sujeitos.

4.4. O produto da atividade de mapeamento de dados pessoais será denominado "Inventário de Dados Pessoais", conforme modelo padronizado no PGP.

4.5. Para efeito desta Diretriz, são deveres do responsável pela unidade organizacional onde os dados pessoais forem tratados:

I - garantir que o inventário de dados pessoais contenha os registros e fluxos de tratamento dos dados, com base na consolidação do mapeamento dos serviços e processos de negócio que realizem o tratamento de dados pessoais, a compreender informações sobre:

a) finalidade do tratamento;

b) base legal;

c) categorias de dados pessoais;

d) identificação das formas de obtenção e coleta dos dados pessoais;

e) categoria dos titulares;

f) fases do ciclo de vida do tratamento;

g) compartilhamento de dados com terceiros, identificando eventual transferência internacional;

h) categorias de destinatários, se houver;

i) prazo de retenção dos dados;

j) medidas de segurança organizacionais e técnicas adotadas; e

k) contratos de serviço ou soluções de Tecnologia da Informação - TI relacionados ao tratamento de dados pessoais.

II - elaborar plano de ação, alinhado com o PGP, para aperfeiçoar as operações de tratamento de dados pessoais mapeadas;

III - identificar lacunas à proteção de dados pessoais nos processos geridos, avaliar os riscos decorrentes e elaborar, sempre que

necessário, o relatório de impacto à proteção de dados pessoais (RIPD);

IV - apresentar ao Gestor de Segurança da Informação a minuta do RIPD com a proposta para tratamento dos riscos e implementar as adequações necessárias e compatíveis conforme orientação daquele Gestor;

V - encaminhar cópia atualizada do inventário de dados pessoais e do RIPD ao Gestor de Segurança da Informação e ao Encarregado pelo Tratamento de Dados Pessoais; e

VI - arquivar o inventário de dados pessoais e os relatórios de impacto à proteção de dados pessoais, permanecendo em condições de disponibilizá-los, em caso de solicitação da ANPD ou de outro órgão de controle.

4.6. Quando o "Inventário de Dados Pessoais" relacionar dados pessoais sensíveis e de crianças e adolescentes, deverão ser adotadas medidas adicionais de proteção e segurança, nos termos do art. 14 da Lei nº 13.709, de 2018.

Capítulo 5 – Relatório de Impacto à Proteção de Dados Pessoais

5.1. O responsável pela unidade organizacional que realizar o tratamento de dados pessoais deverá confeccionar o relatório de impacto à proteção de dados pessoais referente aos atos em que o tratamento de tais dados tenha potencial de gerar risco a direitos e liberdades fundamentais, de acordo com as orientações previstas no PGP e as normas expedidas pela ANPD.

5.2. A elaboração do Relatório de Impacto à Proteção de Dados Pessoais deverá:

I - conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e garantia da segurança das informações, os riscos e as medidas, salvaguardas e mecanismos de mitigação de riscos, conforme modelo estabelecido no PGP;

II - anteceder à celebração de contrato ou convênio que tenha por objeto operações de tratamento de dados pessoais;

III - anteceder ao tratamento de dados pessoais realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, ou quando esse tratamento for realizado com fundamento no legítimo interesse do Ministério da Defesa; e

IV - ocorrer sempre que for demandado pela ANPD, conforme prazo estabelecido.

5.3. Os relatórios de impacto gerados deverão ser mantidos atualizados, no mínimo, anualmente, e arquivados no setor que o originou, que deverá encaminhar uma cópia para o Gestor de Segurança da Informação e para o Encarregado pelo Tratamento de Dados Pessoais.

Capítulo 6 – Medidas de Segurança

6.1. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados. Para tanto, não só os dados registrados em suporte físico, que deverão estar acondicionados em estado e em locais adequados, como também os armazenados em suporte digital devem observar critérios de segurança compatíveis com seu sigilo.

6.2. Cabe ao responsável pela unidade organizacional onde os dados pessoais são tratados implementar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais, ou não, de eliminação, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, nos termos da Lei nº 13.709, de 2018, por meio das seguintes ações:

I - implementação do previsto na Política de Segurança da Informação;

II - adoção de mecanismos de segurança e privacidade, desde a concepção de novos produtos ou serviços (*security by design* e *privacy by design*);

III - elaboração de um plano de resposta a incidentes identificados no relatório de impacto;

IV - avaliação dos sistemas e bancos de dados em que houver tratamento de dados pessoais ou tratamento de dados sensíveis, bem como suas eventuais integrações com outros sistemas, submetendo os riscos identificados, quando não passíveis de tratamento, à apreciação do Gestor de Segurança da Informação, para as orientações necessárias;

V - análise da segurança das hipóteses de compartilhamento de dados pessoais; e

VI - realização de treinamentos.

6.3. O plano de resposta a incidentes envolvendo dados pessoais deverá prever a comunicação imediata do incidente ao Encarregado pelo Tratamento de Dados Pessoais e ao Gestor de

Segurança da Informação, no prazo máximo de vinte e quatro horas, com esclarecimento da natureza do incidente e das medidas adotadas para a apuração das suas causas e a mitigação de novos riscos e dos impactos causados aos titulares dos dados.

6.4. A eliminação de documentos que contenham dados pessoais deverá estar em conformidade com a Tabela de Temporalidade do Ministério da Defesa e com as orientações do Arquivo Nacional, devendo ser realizada de forma a impedir a identificação dos dados pessoais neles contidos, sem prejuízo dos registros documentais correspondentes para fim de rastreamento das medidas adotadas, mediante publicação do ato correspondente em Boletim Interno da ESG.

6.5. A eliminação de documentos de que trata o item 6.4 não afasta os deveres previstos na Lei nº 13.709, de 2018, em relação aos dados pessoais que remanescerem em índices, classificadores, indicadores, banco de dados, arquivos de cópia de segurança ou qualquer outro modo de conservação adotado.

6.6. O responsável pela unidade organizacional armazenará os documentos físicos que contenham dados pessoais e dados pessoais sensíveis de forma segura e com acesso restrito.

Capítulo 7 – Incidentes Envolvendo Dados Pessoais

7.1. As unidades organizacionais responsáveis pelo tratamento de dados pessoais devem monitorar preventivamente os eventos relacionados no relatório de impacto à proteção de dados pessoais, visando evitar incidentes envolvendo dados pessoais.

7.1.1. É dever de todos que tiverem conhecimento de qualquer evento que possa gerar risco às liberdades civis e aos direitos fundamentais de titulares de dados pessoais tratados, informar imediatamente ao Encarregado pelo Tratamento de Dados Pessoais, que proverá as orientações pertinentes, e ao Gestor de Segurança da Informação.

7.1.2. O Encarregado pelo Tratamento de Dados Pessoais providenciará a divulgação no sítio institucional da intranet, na área proteção de dados pessoais, informações e o canal oficial interno para registro de requisições e ocorrências envolvendo o tratamento de dados pessoais.

7.2. Os incidentes de segurança que possam acarretar risco ou dano relevante aos titulares de dados pessoais deverão ser comunicados:

I - ao Encarregado pelo Tratamento de Dados Pessoais e ao Gestor de

Segurança da Informação, no prazo máximo de vinte e quatro horas, com esclarecimento da natureza do incidente e das medidas adotadas para a apuração das suas causas e a mitigação de novos riscos e dos impactos causados aos titulares dos dados, conforme previsto no plano de resposta a incidentes de que trata o item 5.3; e

II - aos titulares de dados pessoais e à ANPD, conforme estabelecido no Plano de Comunicação do Programa de Gestão de Privacidade.

7.2.1. Caberá ao Gestor de Segurança da Informação:

I - dar ciência do incidente ao Comandante da ESG;

II - coordenar as medidas técnicas e administrativas para cessar o incidente;

III - elaborar comunicado de incidente dirigido à ANPD e aos respectivos titulares, observados os prazos estabelecidos e procedimentos adotados pela ANPD; e

IV - acompanhar as medidas afetas ao incidente até o término de seus efeitos.

7.2.2. Caberá às unidades organizacionais responsáveis pelo tratamento de dados pessoais:

I - prestar todas as informações e adotar as medidas necessárias para apurar a natureza dos dados pessoais afetados;

II - informar quais os titulares de dados pessoais foram atingidos pelo incidente; e

III - indicar as medidas técnicas e de segurança utilizadas para a proteção dos dados e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo decorrente do incidente, empregando, sempre que possível, plano de resposta a incidentes previsto no art. 5.3.

7.2.3. Caso as unidades organizacionais responsáveis pelo tratamento de dados pessoais não comuniquem imediatamente o incidente ao Gestor de Segurança da Informação e ao Encarregado pelo Tratamento de Dados Pessoais, será necessário justificar o motivo da demora e as medidas que foram tomadas para reverter ou mitigar os efeitos.

7.3. Caberá às unidades organizacionais responsáveis pelo tratamento de dados pessoais elaborar o relatório de impacto à proteção de dados pessoais específico sobre o incidente, mediante apoio do Gestor de Segurança da Informação e orientação do Encarregado pelo Tratamento de Dados Pessoais.

Capítulo 8 – Adequação de Contratos

8.1. A ESG deverá revisar e adequar todos os contratos que porventura envolvam as atividades de tratamento de dados pessoais às normas de privacidade e proteção de dados pessoais, considerando a responsabilização dos agentes de tratamento prevista na lei, devendo:

I - revisar os modelos existentes de minutas de contratos e convênios externos, proceder aos ajustes nos instrumentos contratuais vigentes e incluir nos novos contratos que envolvam atividades de tratamento de dados pessoais, cláusulas específicas, em especial sobre compartilhamento, retenção e eliminação de dados pessoais, conforme a finalidade pública e a necessidade das operações de tratamento;

II - elaborar, quando necessário, termos de tratamento de dados pessoais para assinatura com os operadores de serviços, incluindo as informações sobre:

a) os dados pessoais que serão tratados;

b) as categorias de titulares dos dados pessoais tratados;

c) as finalidades dos dados pessoais tratados; e

d) os limites do tratamento dos dados pessoais.

III - elaborar orientações e procedimentos para as contratações futuras, em conformidade com a Lei nº 13.709, de 2018; e

IV - criar procedimentos de auditoria regulares para realizar a gestão de terceiros com quem houver o compartilhamento de dados pessoais.

Parágrafo único. A ESG deverá exigir de seus fornecedores de tecnologia, automação e armazenamento a adequação às exigências da Lei nº 13.709, de 2018, quanto aos sistemas e programas de gestão de dados pessoais por eles tratados.

Capítulo 9 – Cultura de Privacidade

9.1. O Plano de Desenvolvimento de Pessoas da ESG deverá prever treinamentos para implementação da cultura de privacidade e proteção de dados pessoais.

Capítulo 10 – Transparência e Direitos dos Titulares

10.1. A Plataforma Integrada de Ouvidoria e Acesso à Informação - *Fala.br* constitui-se no canal oficial para atendimento das requisições e reclamações apresentadas pelos titulares dos dados pessoais.

10.1.1. Todas as demandas recebidas por meio do Fala.br relativas ao atendimento de requisições e reclamações apresentadas pelos titulares dos dados pessoais deverão ser encaminhadas para conhecimento do Encarregado pelo Tratamento de Dados Pessoais, que adotará as seguintes medidas:

I - distribuição do processo, quando aplicável; e

II - acompanhamento do fluxo para atendimento aos direitos dos titulares de dados pessoais, requisições e reclamações apresentadas, desde o seu ingresso até o fornecimento da resposta.

10.1.2. O Encarregado pelo Tratamento de Dados Pessoais deverá manter canal eletrônico específico para orientação aos titulares dos dados pessoais, devendo informar aos titulares de dados pessoais que as demandas oficiais deverão ser direcionadas para o *Fala.br.*

10.2. O responsável pela unidade organizacional que realizar o tratamento de dados pessoais deverá acompanhar o fluxo correspondente durante todo seu ciclo de vida, respeitando os princípios da Lei nº 13.709, de 2018.

10.3. Os responsáveis pelo tratamento de dados pessoais deverão disponibilizar informações adequadas a respeito dos procedimentos de tratamento de dados pessoais, nos termos do art. 9º da Lei nº 13.709, de 2018, por meio de:

I - termos de uso e avisos de privacidade dos serviços e sistemas que tratem dados pessoais; e

II - avisos de cookies nos sítios eletrônicos, quando aplicável.

10.4. Os responsáveis pela unidade organizacional que realizar o tratamento de dados pessoais deverá informar ao Encarregado pelo Tratamento de Dados Pessoais, semestralmente, as categorias de dados tratados e suas finalidades.

10.5. O Encarregado pelo Tratamento de Dados Pessoais encaminhará à Assessoria de Comunicação Social (ACS) da ESG, sempre que houver atualização, as informações para a divulgação, no sítio eletrônico institucional, a respeito dos procedimentos de tratamento de dados, a compreender:

I - categorias de dados tratados e suas finalidades;

II - os direitos dos titulares dos dados;

III - o canal de atendimento disponibilizado aos titulares de dados para que exerçam seus direitos; e

IV - os dados de contato do Encarregado pelo Tratamento de Dados Pessoais.

10.6. Para o tratamento de dados pessoais realizado com fundamento no consentimento do titular, a unidade responsável pelo tratamento deverá prover a rastreabilidade do ciclo de vida destes dados, com a finalidade de possibilitar a revogação do consentimento mediante requisição do titular.

Capítulo 11 – Compartilhamento e Transferência Internacional

11.1. O compartilhamento de dados pessoais com órgãos públicos deverá considerar o disposto no Decreto nº 10.046, de 9 de outubro de 2019 e na Lei nº 13.709, de 2018, em especial os princípios da adequação, da necessidade e a finalidade pública que justificam o compartilhamento, observados os regulamentos e as normas editados pela ANPD.

11.2. Para o compartilhamento de dados pessoais com pessoa de direito privado deverá ser observado o disposto no art. 4º, § 4º, no art. 24, parágrafo único, no art. 26, § 1º, e no art. 27 da Lei nº 13.709, de 2018.

11.3. O compartilhamento de dados com órgãos públicos somente será autorizado nas hipóteses previstas no art. 7º e 11 da Lei nº 13.709, de 2018.

11.3.1. Sempre que possível deverão ser estabelecidos limites ao tratamento de dados pessoais e a responsabilidade dos respectivos agentes de tratamento.

11.3.2. O compartilhamento deverá ser oferecido na modalidade de fornecimento de acesso a informações específicas adequadas, necessárias e proporcionais ao atendimento das finalidades específicas, observados os protocolos de segurança da informação e evitando a transferência de bancos de dados, salvo quando estritamente necessária para o pleno atendimento do interesse público.

11.4. O responsável por compartilhar dados pessoais efetuará, sempre que possível, a criptografia ou a pseudonimização de dados pessoais para o acesso a informações ou transferência dos dados para terceiros, observados os requisitos de segurança da informação, a finalidade do tratamento e a base legal que o autorize.

11.5. A transferência internacional de dados pessoais deverá observar o estabelecido nos art. 33 a 36 da Lei nº 13.709, de 2018, e será regulada por norma específica a ser proposta pela unidade organizacional que realize transferência internacional de dados no âmbito de suas competências.

11.6. As operações de transferência de dados pessoais devem ser informadas para o Encarregado pelo Tratamento de Dados Pessoais, para fins de acompanhamento.

Capítulo 12 – Disposições Finais

12.1 Esta Portaria será publicada em Boletim Interno da Escola Superior de Guerra e disponibilizada em suas páginas da Internet e da Intranet.

ALEXANDRE OLIVEIRA **CANTANHEDE** LAGO
General de Divisão
Comandante