DIÁRIO OFICIAL DA UNIÃO

Publicado em: 02/12/2022 | Edição: 226 | Seção: 1 | Página: 47

Órgão: Ministério da Defesa/Gabinete do Ministro

PORTARIA GM-MD Nº 5.814, DE 29 DE NOVEMBRO DE 2022

Dispõe sobre a Diretriz para a Proteção de Dados Pessoais no Ministério da Defesa.

O MINISTRO DE ESTADO DA DEFESA, no uso das atribuições que lhe confere o art. 87, parágrafo único, incisos I e II, da Constituição, tendo em vista o disposto no art. 5º, inciso VI, da Lei nº 13.709, de 14 de agosto de 2018, e de acordo com o que consta do Processo Administrativo nº 60220.000120/2022-68, resolve:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 1º Esta Portaria dispõe sobre a Diretriz para a Proteção de Dados Pessoais no Ministério da Defesa, exceto quanto às Forças Armadas.

Parágrafo único. Os Comandos da Marinha, do Exército e da Aeronáutica definirão suas diretrizes para a proteção de dados pessoais e exercerão as funções típicas de controlador previstas na Lei nº 13.709, 14 de agosto de 2018.

Art. 2º O Ministério da Defesa exercerá as funções típicas de controlador, subsidiado, no que se refere à dimensão estratégica do assunto, pelo Comitê de Governança do Ministério da Defesa (CG-MD), instituído pela Portaria GM-MD nº 3.127, de 28 de julho de 2021.

Art. 3º Os órgãos que integram o Ministério da Defesa deverão observar as disposições da Lei nº 13.709, de 2018, e aplicar os princípios previstos no seu art. 6º, em toda e qualquer operação de tratamento de dados pessoais que realizarem, independentemente do meio ou do país onde os dados estejam localizados.

Parágrafo único. Deverão ser adotadas as diretrizes, os regulamentos, as normas, as orientações e os procedimentos expedidos pela Autoridade Nacional de Proteção de Dados Pessoais (ANPD), observadas as competências do art. 55-J da Lei nº 13.709, de 2018.

CAPÍTULO II

GOVERNANÇA, GESTÃO E BOAS PRÁTICAS

Art. 4º O tratamento de dados pessoais no âmbito do Ministério da Defesa será promovido de forma a atender à finalidade pública, na busca do interesse público, tendo como objetivos executar suas competências e atribuições legais e normativas.

Art. 5º O Comitê de Governança do Ministério da Defesa (CG-MD) acompanhará, em nível estratégico, as ações relacionadas ao tratamento de dados pessoais, por meio da estrutura de governança estabelecida, competindo-lhe:

I - apreciar propostas de diretrizes e políticas visando à conformidade com as disposições da Lei nº 13.709, de 2018;

II - promover e acompanhar a implementação de medidas e iniciativas para o incremento do nível de maturidade da proteção de dados pessoais;

III - fomentar a cultura de privacidade e proteção de dados pessoais; e

IV - propor aperfeiçoamentos na estrutura de governança estabelecida para o tratamento de dados pessoais.

Art. 6º A gestão das operações de proteção de dados pessoais será orientada e acompanhada:

I - no âmbito da administração central do MD, pelo Comitê de Governança Digital do Ministério da Defesa (CGD-MD); e

II - no âmbito do Hospital das Forças Armadas (HFA), da Escola Superior de Guerra (ESG), da Escola Superior de Defesa (ESD) e do Centro Gestor e Operacional do Sistema de Proteção da Amazônia (CENSIPAM), pelos respectivos comitês internos de governança ou instâncias equivalentes, os quais poderão estabelecer diretrizes e procedimentos complementares para o tratamento de dados pessoais em razão de suas especificidades.

Art. 7º Cabe ao CGD-MD e aos comitês internos de governança ou instância equivalentes do HFA, da ESG, da ESD e do CENSIPAM, no âmbito de suas competências:

I - subsidiar o CG-MD 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 - propor aperfeiçoamentos nas diretrizes, políticas, procedimentos e estruturas relacionados à proteção de dados pessoais.

Art. 8º 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 do Ministério da Defesa.

Parágrafo único. 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.

Art. 9º O PGP deverá considerar as prioridades e as peculiaridades das unidades organizacionais para o cumprimento desta Portaria.

Parágrafo único. Para efeito desta Portaria, unidade organizacional responsável pelo tratamento de dados pessoais corresponde a todo componente da estrutura organizacional do Ministério da Defesa que realize operação de tratamento de dados pessoais.

Art. 10. 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 do Ministério da Defesa 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 III

MAPEAMENTO E INVENTÁRIO DE DADOS PESSOAIS

Art. 11. A unidade organizacional responsável pelo tratamento de dados pessoais deverá realizar o mapeamento e o inventário dos dados pessoais sob sua custódia.

§ 1º 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.

§ 2º O mapeamento de dados pessoais de que trata o caput 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.

Art. 12. O produto da atividade de mapeamento de dados pessoais será denominado "Inventário de Dados Pessoais", conforme modelo padronizado no PGP.

Parágrafo único. Para efeito do caput, 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.

Art. 13. 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 IV

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

Art. 14. 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.

Parágrafo único. 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.

Art. 15. 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 V

MEDIDAS DE SEGURANÇA

Art. 16. 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.

Parágrafo único. 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.

Art. 17. 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 do Ministério da Defesa.

Parágrafo único. A eliminação de documentos de que trata o caput 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.

Art. 18. 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 VI

INCIDENTES ENVOLVENDO DADOS PESSOAIS

Art. 19. 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.

§ 1º 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.

§ 2º 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.

Art. 20. 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 art. 15; e

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

§ 1º Caberá ao Gestor de Segurança da Informação:

I - dar ciência do incidente ao Ministro de Estado de Defesa;

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.

§ 2º 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. 15.

§ 3º 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.

Art. 21. 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 VII

ADEQUAÇÃO DE CONTRATOS

Art. 22. A unidade organizacional deverá revisar e adequar todos os contratos que 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. Os responsáveis pelas unidades organizacionais deverão 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 VIII

CULTURA DE PRIVACIDADE

Art. 23. O Plano de Desenvolvimento de Pessoas da administração central do Ministério da Defesa e os documentos equivalentes da ESG, da ESD, do CENSIPAM e do HFA deverão prever treinamentos para implementação da cultura de privacidade e proteção de dados pessoais.

CAPÍTULO IX

TRANSPARÊNCIA E DIREITOS DOS TITULARES

Art. 24. 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.

§ 1º 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.

§ 2º 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.

Art. 25. 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.

Art. 26. 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.

Art. 27. 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.

Art. 28. O Encarregado pelo Tratamento de Dados Pessoais encaminhará à Assessoria Especial de Comunicação Social do Ministério da Defesa, 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.

Art. 29. 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 X

COMPARTILHAMENTO E TRANSFERÊNCIA INTERNACIONAL

Art. 30. 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.

Parágrafo único. 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.

Art. 31. 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.

§ 1º Sempre que possível deverão ser estabelecidos limites ao tratamento de dados pessoais e a responsabilidade dos respectivos agentes de tratamento.

§ 2º 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.

Art. 32. 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.

Art. 33. A transferência internacional de dados pessoais deverá observar o estabelecido nos arts. 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.

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

CAPÍTULO X

DISPOSIÇÕES FINAIS

Art. 34. Esta Portaria será publicada em Diário Oficial da União e disponibilizada no Portal do Ministério da Defesa e na sua Intranet.

Art. 35. Esta Portaria entra em vigor em 2 de janeiro de 2023.

PAULO SÉRGIO NOGUEIRA DE OLIVEIRA