Diário Oficial
Imprensa Nacional

REPÚBLICA FEDERATIVA DO BRASIL
BRASÍLIA - DF

Nº 122 - DOU – 30/06/22 - Seção 1 – p.145

MINISTÉRIO DA SAÚDE
AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR

RESOLUÇÃO ADMINISTRATIVA ANS Nº 80, DE 28 DE JUNHO DE 2022

Dispõe sobre a Política de Proteção de Dados Pessoais no âmbito da Agência Nacional de Saúde Suplementar.

A DIRETORIA COLEGIADA DA AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR - ANS, no uso da atribuição que lhe confere o inciso II do art. 10 da Lei nº 9.961, de 28 de janeiro de 2000, e tendo em vista o disposto na Lei nº 13.709 de 14 de agosto de 2018, na Lei nº 12.527, de 28 de novembro de 2011, na Lei nº 14.129, de 29 de março de 2021, na Lei nº 9.507, de 12 de novembro de 1997 e no Decreto nº 10.046 de 9 de outubro de 2019, bem como o disposto no Regimento Interno da ANS - Resolução Regimental - RR nº 21, de 26 de janeiro de 2022 e no Guia de Boas Práticas para Implementação na Administração Pública Federal da Lei Geral de Proteção de Dados Pessoais (LGPD), em reunião realizada no dia 24 de JUNHO de 2022, adotou a seguinte Resolução Administrativa, e, eu, Diretor-Presidente, determino a sua publicação:

CAPÍTULO I

DO OBJETIVO E ABRANGÊNCIA

Art. 1º A Política de Proteção de Dados Pessoais (PPDP) da Agência Nacional de Saúde Suplementar (ANS) tem por finalidade estabelecer diretrizes para a proteção dos dados pessoais, observadas a legislação pertinente e as normas e orientações estabelecidas pelo Poder Executivo quanto à privacidade, à proteção dos dados pessoais, à transparência, ao acesso às informações públicas e à proteção das liberdades e dos direitos fundamentais dos indivíduos.

Parágrafo único. Esta Política se aplica aos servidores, colaboradores, terceirizados, estagiários, fornecedores e todos que realizem atividades que envolvam, de forma direta ou indireta, tratamento de dados pessoais custodiados pela Agência, constantes nas suas diferentes bases e sistemas.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 2º Para os fins desta Política, considera-se:

I - 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;

II - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

III - Autoridade Nacional de Proteção de Dados (ANPD): órgão da Administração Pública Federal responsável por zelar, implementar e fiscalizar o cumprimento da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), em todo o território nacional;

IV - compartilhamento de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

V - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - dado anonimizado: dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

VIII - dado pessoal: dado relacionado a pessoa natural identificada ou identificável;

IX - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

X - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XI - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), bem como para orientar a conformidade da organização à LGPD;

XII - inventário de dados pessoais: registro das operações de tratamento dos dados pessoais realizados pelo controlador;

XIII - lei específica: Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) ou outra que venha a substituí-la;

XIV - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

XV - pseudonimização: tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro;

XVI - relatório de impacto à proteção de dados pessoais: documentação do controlador 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;

XVII - termo de uso: documento que estabelece as regras e condições de uso de determinado serviço;

XVIII - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

XIX - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro; e

XX - 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.

CAPÍTULO III

DOS PRINCÍPIOS

Art. 3º Esta Política está pautada nos seguintes princípios no tratamento de dados pessoais:

I - finalidade: o tratamento dos dados deve possuir propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

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

III - necessidade: limitação do tratamento ao mínimo necessário para o alcance da finalidade, considerados apenas os dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - 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;

V - 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 do respectivo tratamento;

VI - 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;

VII - 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;

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

IX - não discriminação: impossibilidade de realização do tratamento de dados pessoais para fins discriminatórios, ilícitos ou abusivos; e

X - 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.

CAPÍTULO IV

DOS FUNDAMENTOS

Art. 4º Esta Política está pautada nos seguintes fundamentos no tratamento de dados pessoais:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

CAPÍTULO V

DAS DIRETRIZES GERAIS

Art. 5º O titular dos dados deverá ter acesso às informações sobre o tratamento de seus dados de forma clara e precisa, nomeadamente sobre o conteúdo, a finalidade e o eventual uso compartilhado, garantido seu livre acesso nos termos da lei específica.

Art. 6º O tratamento de dados pessoais somente deverá ser realizado dentro das hipóteses previstas na lei específica.

Art. 7º Os processos e atividades existentes, relacionados ao tratamento de dados, e aqueles que vierem a ser estabelecidos, deverão ser ajustados com base na limitação do tratamento ao mínimo necessário para a realização de suas finalidades.

Art. 8º Os aplicativos e sistemas da ANS deverão obter a concordância do usuário para o tratamento de seus dados pessoais, inicialmente, pelo conhecimento dos respectivos termos de uso.

§ 1º Os termos de uso de aplicativos e sistemas serão elaborados e mantidos atualizados à luz da lei específica.

§ 2º Ao utilizar o aplicativo ou sistema, o titular do dado pessoal deverá ser informado de forma clara e explícita sobre quais dados serão coletados, a finalidade, a natureza obrigatória ou facultativa do fornecimento e sobre as consequências da negativa em fornecê-los.

Art. 9º Os mecanismos de proteção contra o uso indevido, tentativas de acesso não autorizados, fraudes, danos, sabotagens e roubos de dados adotados no âmbito da Agência deverão ser respeitados por aqueles que se relacionam com a ANS.

Art. 10. As medidas de segurança e proteção de dados pessoais deverão ser priorizadas para minimização dos riscos inerentes às atividades de tratamento de dados pessoais.

Art. 11. Os contratos, convênios e congêneres relacionados a atividades que envolvam tratamento de dados pessoais deverão ser adequados à lei específica.

Art. 12. O compartilhamento de dados dar-se-á nos termos da legislação e normativos vigentes e deverá constar do inventário de dados, bem como dos contratos, convênios e congêneres.

Art. 13. Os procedimentos e o plano de resposta a incidentes relacionados à privacidade dos titulares dos dados deverão ser elaborados a partir de critérios de controle e registro de vazamentos e contemplar o fluxo de comunicação aos envolvidos e à ANPD.

Art. 14. O inventário de dados pessoais deverá ser mantido permanentemente atualizado pela Assessoria de Proteção de Dados e Informações (APDI).

Art. 15. Os regulamentos, serviços, sistemas e aplicativos da ANS que envolvam tratamento de dados pessoais e forem desenvolvidos ou adquiridos deverão seguir os conceitos de privacidade e proteção dos dados pessoais desde a concepção, limitando a coleta de dados pessoais apenas àqueles itens necessários para os propósitos da atuação institucional.

CAPÍTULO VI

DO TRATAMENTO DE DADOS PESSOAIS

Art. 16. O tratamento de dados pessoais pela ANS será realizado para o cumprimento de obrigação legal ou regulatória, para a execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, bem como para a realização de pesquisas, observadas as disposições da lei específica.

Art. 17. Os dados pessoais deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado em cumprimento ao disposto no art. 25 da Lei nº 13.709, de 14 de agosto de 2018, e no art. 8º, § 3º, da Lei nº 12.527, de 18 de novembro de 2011, de forma a facilitar seu uso quando necessário.

Art. 18. Em atendimento a suas competências legais, a ANS poderá, no estrito limite de sua missão institucional, tratar dados pessoais com dispensa de obtenção de consentimento pelos respectivos titulares; sendo que eventuais atividades que transcendam o escopo das obrigações legais, regulatórias e fiscalizatórias estarão sujeitas à obtenção de consentimento dos interessados.

§ 1º Quando o consentimento for a base legal adequada, a ANS deverá garantir que este se dará a partir de clara explicitação da finalidade de uso dos dados concedidos.

§ 2º Nos casos de surgimento de finalidade diversa, deverá ser obtido novo consentimento, mediante adequada e explícita informação da nova finalidade ao titular.

Art. 19. Os dados pessoais tratados pela ANS devem ser:

I - protegidos por procedimentos internos, com trilhas de auditoria para registrar autorizações, utilização, impactos e violações;

II - mantidos disponíveis, exatos, adequados, pertinentes e atualizados, sendo que a retificação ou eliminação do dado deverá ser feito junto à instituição pública ou privada que promoveu o tratamento do dado originalmente;

III - quando coletados diretamente pela ANS serão mantidos disponíveis, exatos, adequados, pertinentes e atualizados, sendo retificado ou eliminado o dado pessoal mediante a constatação de impropriedade respectiva, ou em face da solicitação do titular, devendo o descarte do dado observar as condições e períodos da tabela de temporalidade de retenção de dados aplicável ao caso;

IV - eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação nas hipóteses legais do artigo 16 da LGPD ou em normas específicas;

V - compartilhados para atender finalidades específicas de execução de políticas públicas e atribuição legal com os órgãos e com as entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º da LGPD; e

VI - revistos periodicamente, sendo de imediato eliminados aqueles que já cumpriram sua finalidade de tratamento e por ter se encerrado o seu prazo de retenção.

Art. 20. As informações sobre o tratamento de dados pessoais serão disponibilizadas aos titulares em linguagem clara e simples, com concisão, transparência, inteligibilidade e acessibilidade, na forma da LGPD e da legislação pertinente.

Art. 21. As áreas responsáveis pelo tratamento de dados devem adotar medidas de segurança, técnicas e administrativas fornecidas pela ANS, capazes de proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Art. 22. As áreas responsáveis pelas atividades de tratamento de dados pessoais devem manter registro das operações de tratamento de dados pessoais que realizarem.

Parágrafo único. Toda e qualquer atividade de tratamento de dados pessoais deve ser registrada, desde a sua coleta até a sua exclusão, indicando quais tipos de dados pessoais serão coletados, a base legal que autoriza os seus usos, as suas finalidades, o tempo de retenção, as práticas de segurança de informação implementadas no armazenamento, e com quem os dados podem ser eventualmente compartilhados, segundo o inventário de dados.

CAPÍTULO VII

DOS DIREITOS DO TITULAR DE DADOS PESSOAIS

Art. 23. A ANS deve zelar para que os titulares dos dados pessoais possam usufruir dos direitos assegurados pela LGPD, aos quais a presente Política se reporta, por remissão, sendo os principais:

I - confirmar a existência de tratamento;

II - acessar os dados;

III - solicitar a correção dos dados incompletos, inexatos ou desatualizados;

IV - anonimizar, bloquear ou eliminar os dados desnecessários, excessivos ou tratados em desconformidade;

V - obter informações sobre as entidades públicas ou privadas com as quais a ANS compartilhou seus dados;

VI - solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses; e

VII - solicitar a revogação do consentimento outrora concedido.

CAPÍTULO VIII

DO ATENDIMENTO AO TITULAR DE DADOS PESSOAIS

Art. 24. A ANS deverá manter mecanismos para atendimento aos direitos dos titulares de dados previstos na legislação específica, como a confirmação e acesso a dados, retificação, restrição de tratamento, revogação de consentimento e exclusão de dados, sempre observando os impactos e os direitos do controlador.

Parágrafo único. Em caso de requisição de exclusão, quando couber, será respeitado o prazo de armazenamento mínimo de informações determinado pela legislação.

Art. 25. O Fala.BR - Plataforma Integrada de Ouvidoria e Acesso à Informação será o canal oficial de recebimento dos requerimentos dos titulares de dados pessoais.

Art. 26. Os prazos e procedimentos para exercício dos direitos do titular perante a ANS observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data), da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo), e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .

CAPÍTULO IX

DA TRANSFERÊNCIA INTERNACIONAL DE DADOS

Art. 27. A ANS observará as disposições da LGPD para os casos que implicam transferências internacionais de dados que resultem em compromissos assumidos em acordos de cooperação internacional ou quando as transferências forem necessárias para a execução de políticas públicas ou atribuições legais ou regulatórias desempenhadas pela Agência.

CAPÍTULO X

DAS MEDIDAS DE PROTEÇÃO DOS DADOS PESSOAIS

Art 28. Para proteger os dados do titular a ANS deverá adotar, dentre outras, uma série de medidas, adequadas aos casos e com base em critérios de risco, tais como:

I - criptografia;

II - anonimização e pseudonimização;

III - proteção contra acesso não autorizado a sistemas;

IV - proteção contra acesso físico e lógico;

V - auditoria e log;

VI - monitoramento e detecção;

VII - compromisso de manutenção do sigilo;

VIII - manutenção do Inventário de Dados;

IX - limitação do acesso aos dados pessoais conforme a finalidade da atividade a ser desenvolvida;

X - plano de resposta a incidentes de privacidade;

XI - inclusão de cláusulas de confidencialidade em contratos e aplicação de sanções decorrentes de incidentes;

XII - proteção de dados desde a concepção e por padrão; e

XIII - capacitação dos servidores que tratam dados para atualização permanente sobre medidas de proteção.

Parágrafo único. A quebra do sigilo acarretará a responsabilização do autor nos termos da legislação.

CAPÍTULO XI

DA ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

Art. 29. Os dados anonimizados não serão considerados dados pessoais 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.

Art. 30. A anonimização e a pseudonimização de dados pessoais devem ser realizadas com o propósito de mitigar os riscos de violação de dados.

CAPÍTULO XII

DO COMPARTILHAMENTO DE DADOS PESSOAIS

Art. 31. A ANS, como controlador, somente poderá compartilhar os dados pessoais do titular em estrita observância aos normativos vigentes.

Art. 32. O compartilhamento de dados pessoais será realizado quando estritamente necessário à finalidade pretendida, inclusive com órgãos públicos em ações de política pública, ou em ações de órgãos de controle ou judiciais, para a realização de estudos por órgãos de pesquisa, ou excepcionalmente com entidades privadas, quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres, bem como objetivando a prevenção de fraudes e irregularidades.

§ 1º O compartilhamento de dados pessoais para fins acadêmicos e para a realização de estudos por órgão de pesquisa deverá ser realizado sempre em conformidade com a LGPD, com a legislação correlata em vigor e com as normas e as diretrizes editadas pela ANPD.

§ 2º Os dados pessoais compartilhados devem ser mantidos em ambiente controlado e seguro, garantindo sempre que possível, a anonimização ou pseudonimização, bem como os devidos padrões éticos, a confidencialidade e o sigilo, visando sempre o atendimento à estrita finalidade acadêmica dos estudos e pesquisas.

Art. 33. Os dados pessoais coletados e tratados de forma minimizada pela ANS, em atenção ao princípio da necessidade, podem vir a ser compartilhados pela agência com operadoras setoriais e prestadores de serviços de saúde quando no desempenho de suas atribuições legais, ações regulatórias e fiscalizatórias, resguardados os direitos do titular e os princípios previstos na lei específica.

CAPÍTULO XIII

DA SEGURANÇA E BOAS PRÁTICAS

Art. 34. A ANS dispõe de uma Política de Segurança da Informação que especifica e determina a adoção de um conjunto de medidas técnicas e administrativas de segurança para a proteção de dados contra acessos não autorizados e situações acidentais ou incidentes culposos ou dolosos de destruição, perda, adulteração, compartilhamento indevido ou qualquer forma de tratamento inadequado ou ilícito.

Art. 35. A ANS deve adotar boas práticas e governança capazes de inspirar comportamentos adequados e de mitigar os riscos de comprometimento de dados pessoais, o que envolve um processo progressivo de transformação cultural, a ser apoiado pela alta direção e pelos órgãos de gestão de pessoas diretamente.

Art. 36. As boas práticas adotadas de proteção de dados pessoais e a governança digital implantada devem ser objeto de campanhas informativas na esfera interna da ANS e em seu sítio eletrônico, visando disseminar cultura protetiva e preventiva, com conscientização de todo corpo funcional e sensibilização dos usuários dos serviços prestados pela Agência, no sentido de incorporar o respeito à privacidade e proteção dos dados pessoais nas atividades institucionais cotidianas.

CAPÍTULO XIV

DA GOVERNANÇA EM PRIVACIDADE E GESTÃO DE RISCOS

Art. 37. A governança em privacidade deverá ser integrada à estrutura geral de governança, representada na ANS pelo Comitê de Governança, Riscos e Controles (CGRC).

Art. 38. O gerenciamento e a priorização de riscos relacionados ao tratamento dos dados pessoais deverão utilizar a metodologia adotada pela Política de Gestão de Riscos da ANS, em harmonia com as diretrizes e boas práticas difundidas pelo governo federal.

Art. 39. O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) deve ser revisto e atualizado anualmente ou sempre que existir qualquer tipo de mudança significativa na finalidade do tratamento destes dados, ou que impacte no processo de como esses dados são tratados ou, ainda, motivada por alteração expressiva na quantidade de dados pessoais coletados que afete o tratamento realizados pela ANS.

Art. 40. A elaboração de um único RIPD para todas as operações de tratamento de dados pessoais ou de um RIPD para cada projeto, sistema, ou serviço deve ser avaliada discricionariamente pela ANS de acordo com os processos internos de trabalho.

Art. 41. A presente Política de Privacidade e Proteção de Dados Pessoais deve alinhar-se institucionalmente à Política de Segurança da Informação e à Política de Governança da Informação.

CAPÍTULO XV

RESPONSABILIZAÇÃO

Art. 42. A Diretoria Colegiada da ANS é responsável por aprovar e fazer cumprir esta Política, dispondo de ferramentas e recursos alocados para esse fim.

Art. 43. A APDI é responsável pela implementação, pelo monitoramento, pelas orientações e esclarecimentos de dúvidas acerca desta Política.

Art. 44. A APDI poderá expedir orientações de caráter geral em complemento a esta Política.

Art. 45. Os gestores das unidades organizacionais da ANS são responsáveis pela observância desta Política em suas áreas de atuação.

Art. 46. Quando solicitado, todos os gestores da ANS deverão prestar informações à APDI, relativas ao tratamento de dados pessoais no âmbito das áreas de suas respectivas competências.

CAPÍTULO XVI

DAS DISPOSIÇÕES FINAIS

Art. 47. Esta Política, bem como os documentos editados para o seu cumprimento, devem ser revisados e aperfeiçoados permanentemente, ou quando identificadas mudanças que causem impacto na sua execução.

Art. 48. Os casos omissos desta Resolução Administrativa serão resolvidos pela Diretoria Colegiada.

Art. 49. Esta Política de Privacidade e Proteção de Dados Pessoais entra em vigor em 1º de agosto de 2022.

MAURICIO NUNES DA SILVA
Substituto