Diário Oficial
Imprensa Nacional

REPÚBLICA FEDERATIVA DO BRASIL
BRASÍLIA - DF

Nº 199 - DOU – 19/10/2023 - Seção 1 – p.89

MINISTÉRIO DA SAÚDE
AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA

PORTARIA N° 1.184, DE 17 DE OUTUBRO DE 2023

Institui a Política de Proteção de Dados Pessoais da Agência Nacional de Vigilância Sanitária (Anvisa).

O Diretor-Presidente da Agência Nacional de Vigilância Sanitária, no uso das atribuições que lhe conferi o art. 172, XII, aliado ao art. 203, III, § 3º, do Regimento Interno aprovado pela Resolução de Diretoria Colegiada - nº 585, de 10 de dezembro de 2021, resolve:

CAPÍTULO I

OBJETIVO E ABRANGÊNCIA

Art. 1º A Política de Proteção de Dados Pessoais da Agência Nacional de Vigilância Sanitária tem como objetivo estabelecer, no âmbito da Agência, diretrizes para a proteção dos dados pessoais, para o cumprimento da legislação, normas, orientações e demais atos 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, prestadores de serviço e todos que realizem atividades que envolvam, de forma direta ou indireta, tratamento de dados pessoais custodiados pela Agência.

CAPÍTULO II

CONCEITOS E DEFINIÇÕES

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

I - agentes de tratamento: o controlador e o operador, são os responsáveis pelo tratamento dos dados pessoais, sujeitos às regras da LGPD e à fiscalização da ANPD;

II - 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;

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 (LGPD), em todo o território nacional;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - Comitê de Governança Digital (CGD): instância de apoio à governança interna da Anvisa responsável pelo suporte e assessoramento à DICOL nas ações estratégicas relativas à tecnologia da informação (TI), gestão e segurança da informação e governança digital no âmbito da Agência;

VI - 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;

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

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

IX - 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;

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

XI - 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;

XII - encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados - ANPD;

XIII - equipe de tratamento e resposta a incidentes da Anvisa (ETIR/Anvisa): grupo de servidores com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em rede de computadores da Agência;

XIV - inventário de dados pessoais: registro das operações de tratamento dos dados pessoais realizados pela instituição, descrevendo informações tais como atores envolvidos, finalidade, hipótese de tratamento, previsão legal, dados pessoais tratados, categoria dos titulares, tempo de retenção, instituições com as quais os dados pessoais são compartilhados, transferência internacional de dados e medidas de segurança adotadas.

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

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

XVII - 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;

XVIII - 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;

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

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

XXI - transferência internacional de dados: transferência de dados pessoais para países estrangeiros ou organismo internacional do qual o país seja membro;

XXII - 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

PRINCÍPIOS

Art. 3º As atividades de tratamento de dados pessoais na Anvisa deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para 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 a realização de suas finalidades, com abrangência dos 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 de seu 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 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

DIRETRIZES GERAIS

Art. 4º O titular dos dados deverá ter acesso às informações sobre o tratamento de seus dados, de forma simplificada e gratuita.

Art. 5º A Agência deverá limitar o tratamento de dados dos processos e atividades existentes ao mínimo necessário para realização de suas finalidades.

Art. 6º Quando a base legal do tratamento for o consentimento, os aplicativos e sistemas da Anvisa deverão obter a concordância do titular para o tratamento de dados pessoais, inicialmente, pelo conhecimento de seus termos de uso, através de meios que permitam a coleta transparente e explícita deste consentimento.

Art. 7º Deverá ser garantida a proteção no acesso aos dados nos sistemas informatizados, incluindo autenticação, cadastro e informações correlacionadas ao titular, além de mecanismos de proteção contra o uso indevido, tentativas de acesso não autorizados, fraudes, danos, sabotagens e roubos de dados.

Art. 8º As medidas e os investimentos em segurança e proteção de dados pessoais deverão ser priorizados para minimização dos riscos inerentes às atividades de tratamento de dados pessoais.

Art. 9º Os contratos, convênios e congêneres relacionados a atividades que envolvam tratamento de dados pessoais deverão ser adequados à lei específica.

Art. 10. O compartilhamento de dados dar-se-á nos termos da legislação e normativos vigentes e deverá constar do inventário de dados pessoais, bem como dos contratos, convênios e congêneres, inclusive nos casos de transferência internacional de dados pessoais, considerando o nível de proteção de dados do país estrangeiro ou organismo internacional do qual o país seja membro.

Art. 11. 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 registros de vazamentos e contemplar o fluxo de comunicação aos envolvidos e à ANPD. O processo de gestão de incidentes de dados é iterativo, contínuo e tem por objetivo interromper e/ou minimizar os impactos decorrentes dos incidentes de vazamento ou uso indevido dos dados dos titulares.

Art. 12. O inventário de dados pessoais deverá ser mantido permanentemente atualizado.

Art. 13. Os regulamentos, serviços, sistemas e aplicativos da Anvisa 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 (privacy by design), limitando a coleta de dados pessoais apenas àqueles itens necessários para os propósitos da atuação institucional.

Art. 14. A Anvisa deverá promover a conscientização dos colaboradores acerca das diretrizes e procedimentos de proteção de dados pessoais implementados. As boas práticas adotadas de proteção de dados pessoais e a governança implantada deverão ser objeto de capacitações e campanhas informativas na esfera interna da agência, visando-se a disseminação da cultura protetiva, com a sensibilização dos interessados.

CAPÍTULO V

TRATAMENTO DE DADOS PESSOAIS

Art. 15. Na Anvisa, os dados pessoais são tratados 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, para a tutela da saúde em procedimentos realizados pela Agência, bem como para a realização de pesquisas, observadas as disposições da lei específica.

Parágrafo único. 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. 16. O tratamento de dados, no exercício da atividade regulatória, dar-se-á, dentre outras, das seguintes formas:

I - processamento de pagamentos de multas e tributos recolhidos pela Agência;

II - processamento dos requerimentos de obtenção, alteração e renovação dos registros de produtos e serviços submetidos à vigilância sanitária;

III - processamento dos requerimentos de obtenção de autorizações e certificados de serviços submetidos à vigilância sanitária;

IV - processamento das notificações de queixas técnicas e eventos adversos, além de ações que se desdobrarem em consequência da análise destas notificações;

V - processamento de requerimentos para inspeção e fiscalização sanitária, no âmbito da Agência, além das ações administrativas decorrentes destes procedimentos;

VI - recebimento e processamento de comentários e sugestões às Consultas Públicas e demais instrumentos de participação social;

VII - processamento de solicitações feitas à Agência pelo usuário.

Art. 17. Em atendimento às suas competências legais, a Anvisa 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 titulares.

§ 1º Quando o consentimento for a base legal adequada, a Anvisa deverá garantir que este se dê 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. 18. As áreas responsáveis pelas atividades de tratamento de dados pessoais devem manter registro das operações de tratamento de dados pessoais que realizarem.

§ 1º Toda e qualquer atividade de tratamento de dados pessoais deve ser registrada, desde a sua coleta até a sua exclusão, indicando as informações a serem contempladas no inventário de dados pessoais.

§ 2º O Encarregado apoiará as unidades organizacionais nos procedimentos de elaboração e atualização do inventário de dados pessoais e ficará responsável por sua consolidação e armazenamento.

CAPÍTULO VI

DIREITOS DO TITULAR DE DADOS PESSOAIS

Art. 19. O titular tem direito a obter da Anvisa, em relação aos seus dados pessoais, a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto em legislação específica;

V - eliminação dos dados pessoais tratados com o consentimento do titular;

VI - informação das entidades públicas e privadas com as quais a Anvisa realizou uso compartilhado de dados;

VII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

VIII - revogação do consentimento.

CAPÍTULO VII

ATENDIMENTO AOS TITULARES DE DADOS PESSOAIS

Art. 20. A Anvisa deverá manter mecanismos para atendimento aos direitos dos titulares de dados previstos na legislação específica, 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. 21. 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. 22. Os prazos e procedimentos para exercício dos direitos do titular perante a Anvisa 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 VIII

AGENTES DE TRATAMENTO

Art. 23. A Anvisa, controladora de dados pessoais, e o operador deverão manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Art. 24. O operador deverá realizar o tratamento segundo as instruções fornecidas pela Anvisa, que verificará a observância das próprias instruções e das normas sobre a matéria.

CAPÍTULO IX

MEDIDAS DE PROTEÇÃO DOS DADOS PESSOAIS

Art. 25. Para proteger os dados do titular a Anvisa 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 pessoais;

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.

Art. 26. Os dados pessoais anonimizados não serão considerados dados pessoais, salvo quando o processo de anonimização ao qual foram submetidos for passível de ser revertido.

Parágrafo único. A anonimização definitiva de dado pessoal será sempre irreversível, sendo aplicada nos casos em que o tratamento do dado pessoal não é mais necessário para atendimento de finalidade pública e o registro não possa ser descartado definitivamente sem comprometer a consistência do sistema ou de outros dados dependentes.

Art. 27. A anonimização de dados pessoais deve ser realizada com o propósito de mitigar os riscos de violação de dados.

Art. 28. Antes de realizar a anonimização de dados pessoais, será verificado se, no ciclo devido de tratamento dos dados, são observados os princípios da finalidade, adequação, necessidade e qualidade dos dados.

CAPÍTULO X

GERENCIAMENTO DE INCIDENTES

Art. 29. Os procedimentos e o plano de resposta a incidentes relacionados à privacidade dos titulares dos dados deverão:

I - ser elaborados a partir de critérios de controle;

II - considerar os registros de vazamentos e sua criticidade;

III - contemplar o fluxo de comunicação aos envolvidos e à ANPD.

Parágrafo único. O gerenciamento de incidentes com dados pessoais deve ter como objetivo principal a cessação ou minimização dos impactos e do uso indevido, decorrentes dos incidentes de vazamento.

Art. 30. Os fornecedores de serviços de Tecnologia da Informação e Comunicação (TIC), na qualidade de operadores de tratamento de dados pessoais, deverão:

I - apresentar evidências e garantias suficientes de que aplica adequado conjunto de medidas técnicas e administrativas de segurança, para a proteção dos dados pessoais, segundo a legislação, os instrumentos contratuais e de compromissos;

II - manter os registros de tratamento de dados pessoais que realizar, com condições de rastreabilidade e de prova eletrônica a qualquer tempo;

III - comunicar formalmente e de imediato à Anvisa a ocorrência de qualquer risco, ameaça ou incidente de segurança que possa acarretar comprometimento ou dano potencial ou efetivo a titular de dados pessoais, evitando atrasos por conta de verificações ou inspeções;

IV - descartar de forma irrecuperável, ou devolver para Anvisa, todos os dados pessoais e as cópias existentes, após a satisfação da finalidade respectiva ou o encerramento do tratamento por decurso de prazo ou por extinção de vínculo legal ou contratual.

Art. 31. A Anvisa estabelecerá, em normativo próprio, o procedimento relativo ao gerenciamento de incidentes de dados pessoais, em consonância com outros procedimentos relacionados à segurança da informação e privacidade.

CAPÍTULO XI

SEGURANÇA E BOAS PRÁTICAS

Art. 32. As medidas técnicas e administrativas de segurança para a proteção de dados pessoais contra acessos não autorizados, situações acidentais, incidentes culposos ou dolosos de destruição, perda, adulteração, compartilhamento indevido ou qualquer forma de tratamento inadequado ou ilícito, deverão seguir o disposto na Política de Segurança da Informação e Comunicação da Anvisa (POSIC).

Art. 33. A Anvisa deve adotar boas práticas de governança em segurança da informação visando orientar comportamentos adequados e mitigar os riscos de comprometimento dos dados pessoais tratados em suas atividades finalísticas e administrativas.

§ 1º A Anvisa deve utilizar ferramentas de tecnologia da informação que sejam aderentes, por padrão e desde a concepção, às boas práticas em segurança da informação e privacidade.

§ 2º Os sistemas de informação em uso na data da publicação desta norma devem ser gradativamente adaptados ao disposto nesta Política, conforme a priorização do Comitê de Governança Digital, observando a conveniência e oportunidade para o órgão e os riscos potenciais e efetivos para a proteção dos dados pessoais envolvidos.

§ 3º As boas práticas adotadas de proteção de dados pessoais e a governança implantada deverão ser objeto de campanhas informativas na esfera interna da Anvisa e em seu sítio eletrônico, visando a disseminar cultura protetiva, com conscientização e sensibilização dos interessados.

CAPÍTULO XII

COMPETÊNCIAS

Art. 34. Compete ao Diretor-Presidente da Anvisa:

I - assegurar que as diretrizes, prioridades e ações específicas de proteção de dados pessoais sejam implementadas na Anvisa;

II - garantir os recursos necessários para a execução da Política de Proteção de Dados Pessoais da Anvisa; e

III - designar o Encarregado pelo Tratamento de Dados Pessoais da Anvisa.

Art. 35. Compete ao Comitê de Governança Digital da Anvisa:

I - aprovar as alterações na Política de Proteção de Dados Pessoais da Anvisa; e

II - aprovar o plano de trabalho do Comitê de Governança Digital referente às atividades de proteção de dados pessoais.

Art. 36. Compete ao Encarregado pelo tratamento de dados pessoais da Anvisa:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da ANPD e adotar providências;

III - orientar a Anvisa e o seu corpo funcional, bem como os contratados da entidade, a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

IV - manter esta Política e suas normas complementares atualizadas e disponíveis na intranet e/ou no sítio eletrônico da Anvisa;

V - promover a divulgação desta Política e das normas complementares, de forma ampla e acessível, a todos os servidores, colaboradores, fornecedores, prestadores de serviços e estagiários que oficialmente executem atividades vinculadas à Anvisa;

VI - coordenar a revisão desta Política e a elaboração das normas complementares dela decorrentes;

VII - acompanhar os trabalhos da ETIR/Anvisa nos incidentes relacionados à proteção de dados pessoais;

VIII - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação de dados pessoais; e

IX - executar as demais atribuições determinadas pela Anvisa ou estabelecidas em normas complementares ou da ANPD.

§ 1º O Diretor-Presidente da Anvisa designará o Encarregado pelo Tratamento de Dados Pessoais.

§ 2º O Encarregado poderá solicitar o apoio de qualquer unidade organizacional para o desempenho de suas atribuições.

§ 3º A identidade e as informações de contato do Encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, no sítio eletrônico da Anvisa.

Art. 37. As unidades organizacionais da Anvisa terão as seguintes responsabilidades:

I - prestar as informações demandadas pelo Encarregado;

II - cumprir as disposições desta Política e as normas complementares dela decorrentes; e

III - definir os seus procedimentos internos em observância à Política de Proteção de Dados Pessoais da Anvisa e suas normas complementares.

Art. 38. Os assuntos referentes à proteção de dados pessoais serão submetidos ao Comitê de Governança Digital da Anvisa, e deverão observar as suas regras e estrutura de governança, ressalvadas as competências específicas do Encarregado.

CAPÍTULO XIII

ATUALIZAÇÕES

Art. 39. Esta Política de Proteção de Dados Pessoais deve ser revisada e atualizada periodicamente, no máximo a cada 2 (dois) anos.

CAPÍTULO XIV

DISPOSIÇÕES FINAIS

Art. 40. Os agentes de tratamento que intervenham em quaisquer fases do tratamento deverão zelar pela segurança da informação, em relação aos dados pessoais, prevista nesta Política.

Art. 41. Os casos omissos serão resolvidos pelo Comitê de Governança Digital.

Art. 42. Esta Política entra em vigor na data de sua publicação.

ANTONIO BARRA TORRES
Diretor-Presidente