STM SUPERIOR TRIBUNAL MILITAR
DIDOC/COGES/LEGIS

Publicado no BJM nº 49-2º
Aditamento, de 29/12/2023

PODER JUDICIÁRIO
SUPERIOR TRIBUNAL MILITAR

ATO NORMATIVO Nº 692

Dispõe sobre o Plano Operacional de Gestão e de Privacidade de Dados Pessoais da Justiça Militar da União.

O MINISTRO-PRESIDENTE DO SUPERIOR TRIBUNAL MILITAR, no uso das atribuições que lhe são conferidas pelo inciso XXV do art 6º do Regimento Interno; e

CONSIDERANDO a Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD), e

CONSIDERANDO a Resolução nº 340, de 27 de novembro de 2023, que "*institui a Política de Governança Arquivística, da Informação, dos Dados e do Conhecimento, no âmbito da Justiça Militar da União*",

R E S O L V E:

Art. 1º Fica instituído o Plano Operacional de Gestão e de Privacidade de Dados Pessoais da Justiça Militar da União (JMU).

Art. 2º Para os efeitos deste Ato Normativo, consideram-se:

I - dado pessoal: aquele relativo a uma pessoa identificada ou identificável, ou seja, não apenas as informações que identificam diretamente uma pessoa (ex.: nome, CPF, RG), mas também as que, tratadas dentro de um contexto, em conjunto com outras informações, permitem a identificação de uma pessoa (ex.: profissão, endereço, sexo, idade);

II - 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;

III - 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;

IV - confidencialidade: propriedade de que a informação não esteja disponível ou não seja revelada a pessoa física, a sistema, a órgão ou a entidades não autorizadas ou não credenciadas;

V - controlador: pessoa jurídica de direito público a quem compete definir todas as ações relativas ao tratamento dos dados pessoais, cuja função não poderá ser exercida por pessoas naturais que atuem como profissionais subordinados a uma pessoa jurídica ou como membros de seus órgãos;

VI - encarregado: pessoa física ou jurídica responsável por, entre outras atribuições, realizar a comunicação entre a Autoridade Nacional de Proteção de Dados, os titulares dos dados e o controlador, bem como conhecer, detalhadamente, todo o tratamento efetivado de dados pessoais na instituição;

VII – Autoridade Nacional de Proteção de Dados Pessoais: órgão vinculado à Presidência da República, ao qual caberá, entre outras atribuições, fiscalizar a aplicação da Lei Geral de Proteção de Dados (LGPD) nas entidades do poder público e aplicar sanções, em caso de descumprimento de suas determinações;

VIII - operador: pessoa física ou jurídica de direito público ou privado que

realiza o tratamento em nome do controlador, cuja atividade não poderá recair sobre subordinados, tais como magistrados, servidores públicos ou equipes de trabalho que já atuam diretamente sob o poder diretivo do controlador e o integram, expressando a atuação deste;

IX - segurança da informação: conjunto de medidas e de ações necessárias para garantir que a autenticidade, a confidencialidade, a integridade e a disponibilidade das informações de uma organização ou de um indivíduo sejam preservadas; e

X – tratamento dos dados: qualquer atividade pertencente ao ciclo de vida dos dados pessoais.

CAPÍTULO I
DA PROTEÇÃO DOS DADOS PESSOAIS

Art. 3º Caberá aos órgãos da JMU, observado o disposto neste Ato Normativo e nas demais normas aplicáveis, assegurar:

I - gestão transparente da informação, propiciando seu amplo acesso e divulgação;

II - proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade; e

III - proteção da informação sigilosa e da privacidade dos dados pessoais, observada sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

Art. 4º Os documentos, os processos e os dossiês, em formato físico ou digital, contendo informações pessoais relativas à intimidade, à vida privada, à honra e à imagem produzidos na JMU serão de acesso restrito ao agente público legalmente autorizado e à pessoa a que se referem.

Art. 5º Na hipótese de tramitação física, o documento, o processo ou o dossiê de acesso restrito será acondicionado em invólucro lacrado.

§ 1º O servidor que detiver a carga do documento, processo ou dossiê adotará as providências necessárias à salvaguarda do sigilo.

§ 2º Se a tramitação física ocorrer no âmbito da mesma unidade administrativa, poderão ser adotados, a critério do titular, procedimentos diversos do previsto no *caput* deste artigo.

Art. 6º Na tramitação digital, os sistemas utilizados deverão:

I - restringir o acesso ao servidor ou ao magistrado a dados desnecessários para manifestação ou ciência; e

II - omitir, na hipótese de pesquisa realizada por usuário interno e/ou externo, as informações que possam comprometer a intimidade, a vida privada, a honra ou a imagem da pessoa a que se referem.

Art. 7º Os servidores das unidades administrativas que custodiem ou tratem informações pessoais com restrição de acesso são autorizados, independentemente de credenciamento, a acessá-las e a geri-las em suas áreas de competência.

CAPÍTULO II
DOS PRINCÍPIOS

Art. 8º Deverão ser considerados os seguintes princípios no tratamento de dados pessoais e em todas as ações relativas a ele:

I - boa-fé: convicção de agir com correção e em conformidade com o Direito;

II - finalidade: tratamento dos dados com propósitos legítimos, específicos, explícitos e informados;

III - adequação: tratamento dos dados compatível com a finalidade pela qual são tratados;

IV - necessidade: limitação do tratamento ao mínimo necessário para o alcance da finalidade, considerados apenas os dados pertinentes, proporcionais e não excessivos;

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

VI - 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;

VII - transparência: garantia aos titulares de informações claras, precisas e

acessíveis sobre o tratamento de seus dados pessoais e sobre os agentes de tratamento;

VIII - segurança e prevenção: utilização de medidas técnicas e administrativas que garantam a proteção dos dados pessoais contra acessos não autorizados e a prevenção contra situações acidentais ou ilícitas que gerem destruição, perda, alteração, comunicação ou difusão desses dados; e

IX - não discriminação: vedação de realizar o tratamento de dados pessoais para fins discriminatórios, ilícitos ou abusivos.

CAPÍTULO III

DO TRATAMENTO DOS DADOS PESSOAIS

Art. 9º O Tribunal poderá realizar o tratamento mínimo dos dados pessoais, necessário e imprescindível à garantia do interesse público e à execução de suas funções jurisdicional e administrativa.

Art. 10. O tratamento dos dados pessoais deverá ser realizado durante todo o ciclo de vida dos documentos.

Parágrafo único. Para a eliminação dos dados pessoais, será utilizado o Plano de Classificação e a Tabela de Temporalidade da JMU.

Art. 11. As informações sobre o tratamento de dados pessoais deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com o uso de recursos audiovisuais, quando necessário, de forma a proporcionar a informação adequada.

Art. 12. Os documentos, os processos e os dossiês deverão conter apenas as informações pessoais necessárias à identificação dos titulares e à prática de atos cuja execução seja indispensável.

Parágrafo único. Para o cumprimento do disposto no *caput* deste artigo, os órgãos e as unidades administrativas deverão adequar os formulários de solicitação de serviços e os relatórios gerados pelos sistemas de informação.

Art. 13. Identificada a necessidade de processamento técnico de informação pessoal por estagiário ou por empregado de entidade privada que possua vínculo contratual com a JMU, serão exigidos:

I - a lavratura de termo de credenciamento pela autoridade competente, que poderá ser substituída pela autorização de acesso, no caso de sistemas informatizados; e

II - a assinatura de termo de responsabilidade, pelo qual se comprometam a resguardar o sigilo das informações a que têm acesso por força de suas atribuições profissionais.

CAPÍTULO IV

DAS RESPONSABILIDADES

Art. 14. Compete ao controlador:

I - realizar a governança e fornecer as instruções para a política de privacidade dos dados pessoais;

II - garantir a observância das instruções e das normas sobre proteção de dados pessoais na JMU;

III - incentivar a disseminação da cultura da privacidade de dados pessoais na JMU;

IV - determinar a permanente atualização deste plano operacional e o desenvolvimento dos respectivos programas; e

V - manter pública a informação sobre os tipos de dados coletados e a forma de sua utilização.

Art. 15. Compete ao encarregado:

I - atuar como canal de comunicação entre a Justiça Militar da União, o titular de dados pessoais e a Autoridade Nacional de Proteção de Dados Pessoais.

II - prestar esclarecimentos, realizar comunicações, orientar operadores e contratados sobre as práticas a serem adotadas para garantir a proteção dos dados pessoais;

III - apoiar a implementação e a manutenção de práticas de conformidade à legislação sobre o tratamento de dados pessoais;

IV - determinar a publicidade da dispensa de consentimento para o tratamento de dados pessoais;

V - receber as reclamações dos titulares quanto ao tratamento de seus dados pessoais, respondê-las e tomar providências para sanar os desvios;

VI - realizar o atendimento dos titulares de dados pessoais internos e externos à JMU; e

VII - manter a comunicação sobre o tratamento de dados pessoais com as autoridades internas e externas à JMU.

Art. 16. Compete ao Comitê Executivo de Privacidade e Dados Orgânicos Abertos - CESDA:

I - elaborar e submeter ao Comitê de Governança de Tecnologia da Informação e Comunicação estudos sobre planejamento, controle e ações de segurança cibernética;

II - formular e conduzir diretrizes para o Sistema de Gestão de Segurança Cibernética e da Informação, considerando as disposições da Lei Geral de Proteção de Dados Pessoais;

III - elaborar diretrizes para o tratamento adequado dos dados pessoais em cadastros, bases de dados e sistemas da JMU visando à proteção desses dados;

IV - elaborar relatório de impacto para proteção de dados pessoais, que deverá descrever os processos de tratamento de dados que possam gerar riscos às liberdades civis e aos direitos fundamentais dos titulares, bem como conter medidas, salvaguardas e mecanismos de mitigação desses riscos;

V - propor ações de tratamento de dados pessoais;

VI - promover, coordenar e acompanhar as ações relacionadas à privacidade dos dados pessoais;

VII - manter interlocução com os demais comitês e unidades administrativas da JMU, a fim de conciliar a execução das ações de segurança cibernética e da informação;

VIII - acompanhar regulamentações no âmbito do Poder Judiciário e monitorar o cumprimento das determinações provenientes da Autoridade Nacional de Proteção de Dados (ANPD) referentes ao tratamento e proteção de dados pessoais; e

IX - propor critérios de classificação das informações administrativas, a fim de que possam ter tratamento diferenciado, conforme seu grau de importância, criticidade, dados sensíveis e necessidade de compartilhamento.

CAPÍTULO V

DOS DADOS PESSOAIS SENSÍVEIS E ANONIMIZAÇÃO

Art. 17. O tratamento de dados pessoais sensíveis somente poderá ocorrer quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas.

Parágrafo único. Os dados pessoais sensíveis receberão um nível maior de proteção, considerando o potencial inerente de gerar discriminação a seus titulares.

Art. 18. O uso compartilhado de dados pessoais sensíveis somente poderá ocorrer após autorização do controlador dos dados.

Art. 19. Na realização de estudos em saúde pública, as unidades administrativas poderão ter acesso a bases de dados pessoais, que serão tratadas exclusivamente dentro da JMU e estritamente para a finalidade de realização de estudos e pesquisas.

§ 1º Os dados pessoais tratados nos termos do *caput* deste artigo deverão ser mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico, que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

§ 2º A divulgação dos resultados ou de qualquer excerto da pesquisa de que trata o *caput* deste artigo, em nenhuma hipótese, poderá revelar dados pessoais.

§ 3º Para os efeitos deste artigo, a pseudonimização é o 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.

§ 4º Os dados anonimizados não são considerados dados pessoais, nos termos do art. 12 da Lei Geral de Proteção de Dados, salvo quando o processo de anonimização ao qual foram submetidos for revertido.

CAPÍTULO VI

DA DIVULGAÇÃO

Art. 20. O Superior Tribunal Militar deverá publicar, em local de fácil acesso e visualização, em seu portal na internet:

I - as hipóteses que fundamentam a realização do tratamento de dados pessoais;

II - a previsão legal, a finalidade e os procedimentos para o tratamento de dados pessoais;

III - a identificação do controlador e do encarregado, com os respectivos contatos de correio eletrônico;

IV - as responsabilidades dos operadores envolvidos no tratamento; e

V - os direitos do titular, com menção expressa ao art. 18 da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados.

Art. 21. A publicidade de informações é preceito geral, sendo o sigilo a exceção, conforme art. 3º, inciso I, da Lei nº 12.527, de 18 de novembro de 2011.

Art. 22. Qualquer falha na segurança da informação relacionada à garantia ou ao controle de acesso, identificada por qualquer usuário, deverá ser, imediatamente, comunicada ao seu superior imediato, que encaminhará à Diretoria de Tecnologia da Informação (Ditin), para avaliação e determinação de ações corretivas.

Art. 23. Os dados pessoais dos magistrados, servidores civis e militares, estagiários e terceirizados relativos à remuneração deverão ser disponibilizados no Portal da Transparência da Justiça Militar da União.

Parágrafo único. Na publicidade da remuneração, os nomes dos magistrados, servidores civis e militares, estagiários e terceirizados deverão ser anonimizados pela matrícula e incluir cargo e lotação.

Art. 24. Os dados pessoais coletados pela recepção nos Órgãos da JMU deverão ser eliminados em 30 (trinta) dias.

Parágrafo único. Na ocorrência de visitação ao Superior Tribunal Militar, caso o visitante se reúna com o Ministro-Presidente, o Diretor-Geral da Secretaria do STM ou o Secretário da Presidência, seu nome poderá ser divulgado na agenda pública.

Art. 25. Os dados coletados, por ocasião da celebração de contratos com a JMU, poderão ser divulgados, mas limitados ao tratamento mínimo necessário.

CAPÍTULO VII

DA CLASSIFICAÇÃO, DO SIGILO DA INFORMAÇÃO, DA GARANTIA E DO CONTROLE DE ACESSO

Art. 26. A classificação da informação tem por objetivo assegurar-lhe um nível adequado de proteção.

§ 1º A informação deverá ser classificada por quem a gerou, a fim de indicar a necessidade, as prioridades e o nível esperado de proteção durante todo o seu ciclo de vida.

§ 2º Toda informação não classificada terá caráter ostensivo e deverá ser fornecida a qualquer cidadão identificado que a solicitar, em formato aberto, independentemente de motivação, exceto a coberta por segredo de justiça ou outro caráter de sigilo.

Art. 27. As informações produzidas por usuários no exercício de suas funções são patrimônio intelectual da JMU, e não cabe a seus criadores qualquer forma de restrição de acesso.

Parágrafo único. Quando as informações forem produzidas por colaboradores para uso exclusivo da JMU, instrumento próprio estabelecerá as obrigações dos criadores, inclusive no que se refere a eventual confidencialidade.

Art. 28. O processo de controle de acesso à informação tem por objetivo garantir que o acesso físico e lógico à informação seja franqueado, exclusivamente, a pessoas autorizadas, com base nos requisitos de negócio e de segurança cibernética e da informação.

§ 1º O acesso às informações não públicas produzidas ou custodiadas pela JMU deverá permanecer restrito às pessoas que tenham necessidade de conhecê-las.

§ 2º O acesso às informações não públicas por quaisquer colaboradores é condicionado ao aceite de termo de sigilo e de responsabilidade.

§ 3º O acesso às informações produzidas ou custodiadas pela JMU submete quem as acessa a controles administrativos e tecnológicos definidos de acordo com a respectiva

classificação.

Art. 29. Todos os usuários que manipulem ou tenham acesso a informações identificadas como sigilosas, sob custódia ou de propriedade da JMU deverão garantir a confidencialidade e o segredo dessas informações.

Parágrafo único. É vedada qualquer forma de impressão, transmissão, compartilhamento ou transporte de informação sigilosa para fora das instalações da JMU sem a devida autorização.

Art. 30. A inobservância dos dispositivos deste Ato Normativo poderá acarretar, isolada ou cumulativamente, nos termos da lei, sanções administrativas, civis ou penais.

Art. 31. Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pela JMU deverão observar, no que couber, as disposições deste Ato Normativo.

CAPÍTULO VIII

DAS DISPOSIÇÕES FINAIS

Art. 32. Os casos omissos serão resolvidos pelo Ministro-Presidente, ouvido o Comitê Executivo de Privacidade, Segurança Cibernética e Dados Abertos.

Art. 33. Este Ato Normativo entra em vigor na data de sua publicação.

Ten Brig Ar **FRANCISCO JOSELI PARENTE CAMELO**

Ministro-Presidente

Documento assinado eletronicamente por **FRANCISCO JOSELI PARENTE CAMELO**, **MINISTRO-PRESIDENTE DO SUPERIOR TRIBUNAL MILITAR**, em 22/12/2023, às 17:14 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.stm.jus.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **3539907** e o código CRC **DFBDDF2C**.

Setor de Autarquias Sul, Praça dos Tribunais Superiores - Bairro Asa Sul - CEP 70098-900 - Brasília - DF - http://www.stm.jus.br/