



**MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO**

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPD

Rio de janeiro, 11 de junho de 2024

Histórico de Revisões

Data	Versão	Descrição	Autor
10/06/2024	1.0	Conclusão da primeira versão do relatório	1º Ten Esp Aer COM Alex Ribeiro Pereira
08/07/2024	1.1	Alteração do Encarregado Setorial	1º Ten Esp Aer COM Alex Ribeiro Pereira

OBJETIVO
O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os processos de tratamento de dados pessoais que podem gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.
Referência: Art. 5º, XVII da Lei 13.709/2018 (LGPD).

1 IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARGADO

Controlador Setorial:	
Departamento de Controle do Espaço Aéreo (DECEA) Ten Brig Av Alcides Teixeira Barbacovi	
Encarregado Setorial:	
Brig Eng André Eduardo Jansen	
E-mail encarregado:	Telefone encarregado:
jansenaej@decea.mil.br	(21) 2101-6460

Art. 5º Para fins desta Lei, considera-se:

VI – Controlador: nome da pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (LGPD, art. 5º, VI);

VII – Encarregado: nome da 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 (LGPD, art. 5º, VIII).

2 NECESSIDADE DE ELABORAR O RELATÓRIO

No caso do DECEA, especificamente nas tratativas do sistema de Solicitação de Acesso de Aeronaves Remotamente Pilotadas (SARPAS), <https://sarpas.decea.mil.br>, o RIPD foi elaborado e atualizado, por existir a possibilidade de ocorrer (mesmo esporadicamente) impacto na privacidade dos dados pessoais, resultante de:

- Uma tecnologia, serviço ou outra nova iniciativa em que os dados pessoais (normais e sensíveis) sejam ou devam ser tratados;
- Tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa

nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais (LGPD, art. 4º, § 3º);

- Tratamento no interesse legítimo do controlador (LGPD, art. 10, § 3º);
- Alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados etc.; e
- Reformas administrativas que implicam em nova estrutura organizacional resultante da incorporação, fusão ou cisão de órgãos ou entidades.

3 DESCRIÇÃO DO TRATAMENTO

A descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais envolve a especificação da **natureza, escopo, contexto e finalidade** do tratamento.

A LGPD (art. 5º, X) considera 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 objetivo principal desta descrição é fornecer cenário institucional relativo aos processos que envolvem o tratamento dos dados pessoais, fornecendo subsídios para avaliação e tratamento de riscos.

3.1 NATUREZA DO TRATAMENTO

Para atender a missão do SARPAS, conforme supracitado, há a necessidade de coleta de dados pessoais dos usuários para as tratativas de identificação, verificação das permissões das solicitações, consultar junto à ANAC as aeronaves de sua responsabilidade e poder realizar notificações.

A partir da integração com órgãos governamentais, coleta-se os seguintes dados:

- a) Autenticação de acesso ao sistema a partir do GOV.BR: nome completo, nome social, foto, CPF, e-mail, telefone e data de nascimento;
- b) Agência Nacional da Aviação CIVIL (ANAC): CPF e as aeronaves (UA) vinculadas ao usuário (sistema SISANT da ANAC);
- c) Além dos dados dos órgãos supracitados, a partir do próprio sistema SARPAS obtêm-

se os seguintes dados: vínculo com organizações e localização a partir das áreas solicitadas.

Os dados são armazenados e mantidos (manutenção, monitoramento e suporte) pela infraestrutura de TI do DECEA (Destacamento de Controle do Espaço Aéreo e Telemática do Rio de Janeiro (DTCEATM-RJ) e pela Assessoria de Transformação Digital do DECEA (ATD)).

Os dados pessoais dos usuários são tratados em ambiente digital sob as premissas tecnológicas de automação e segurança da informação (backup, testes automatizados, firewall, DMZ, etc).

3.2 ESCOPO DO TRATAMENTO

O tratamento dos dados do sistema SARPAS tem abrangência nacional.

Para essa atividade, há a necessidade dos tratamentos abaixo:

- a) Dados pessoais sensíveis obtidos a partir da autenticação do GOV.BR como a identificação dos usuários (nome, identidade, CPF, etc);
- b) Vinculação das aeronaves (disponibilizado a partir de API da ANAC – a partir do sistema SISANT); e
- c) Vínculos com organizações e localização do Drone a partir das áreas solicitadas (a partir do sistema SARPAS).

O sistema possui mais de 124.210 titulares do sistema anualmente.

Os dados são obtidos, tratados ou atualizados conforme o acesso dos usuários ao sistema, sendo que o período de retenção das informações segue as regulamentações da Lei.

Além disso, deve-se ressaltar a necessidade da manutenção das identificações dos voos para fins de auditoria e rastreabilidade.

3.3 CONTEXTO DO TRATAMENTO

No caso do SARPAS, como descrito na identificação da necessidade de elaborar o presente Relatório de Impacto, o contexto do tratamento de dados pessoais está relacionado à execução de regulamentos e políticas públicas, devidamente previstas em lei.

Diante da natureza do relacionamento do SARPAS com os usuários, com a finalidade supracitada, destaca-se que os dados sensíveis e os dados das aeronaves são obtidos das fontes governamentais. Logo, os indivíduos poderão controlar os seus dados pessoais a partir das fontes dos dados (GOV.BR e ANAC), pois o SARPAS só consulta os dados.

O SARPAS não realiza tratamento de grupos vulneráveis (crianças e adolescentes, entre outros).

Os dados pessoais obtidos são tratados conforme determinação das leis e regulamentos, e comunicado pela instituição ao titular de dados.

Em razão do objeto do sistema e da importância que o mesmo possui nas operações do DECEA e na segurança de voo de nosso país, não é possível solicitar a exclusão de seus dados pessoais de nossa base.

3.4 FINALIDADE DO TRATAMENTO

O SARPAS visa cumprir as obrigações legais e regulatórias do DECEA, assim atender as políticas públicas, o direito jurídico, a necessidade de gerenciamento dos Drones para a execução segura dos voos dos usuários perante os órgãos de Controle do Espaço Aéreo. Diante disso, o sistema prove autorizações dos voos dos Drones para garantir os seguintes serviços:

1. Integridade/singularidade dos dados do usuário (dados pessoais como o nome e CPF);
2. Realizar contato com o usuário, se necessário (a partir de e-mail e telefones).

4 PARTES INTERESSADAS CONSULTADAS

O DECEA possui uma parceria de compartilhamento das tecnologias digitais com a ANAC e é integrado ao serviço governamental - GOV.BR, sendo realizado compartilhamento de dados de forma segura via API.

5 NECESSIDADE E PROPORCIONALIDADE

O DECEA visando a adoção de medidas para a proteção da segurança, confidencialidade e integridade do processo de tratamento de dados pessoais durante a estruturação do sistema SARPAS preconizou a compatibilidade dos seus dados com entidades governamentais certificadas.

Essa ação foi aplicada com a finalidade de validar o acesso dos usuários e obter dados sensíveis com o ganho de segurança e rastreabilidade a partir da autenticação pelo GOV.BR, além de desonerar o DECEA da guarda dos dados pessoais dos usuários, já que os dados cadastrais são guardados pelo SERPRO.

Além disso, ratificando a necessidade da integridade dos dados, utiliza-se a integração com a ANAC (a partir de API) para obtenção de dados relacionados às aeronaves autorizadas para uso pelos usuários.

Ressalta-se que a utilização dos dados pessoais será limitada, sendo tratados somente os dados essenciais para a execução das regras de negócio da aplicação, conforme preconiza a LGPD, art. 6º, III.

A ação tem como fundamento legal o legítimo interesse do controlador (LGPD, art. 10), pois o tratamento de dados é imprescindível para identificação e designação das autorizações de voo, a base do GOV.BR é a mais fidedigna e não há outra base legal possível de se utilizar para alcançar o mesmo propósito, além desse processamento ser imprescindível para o propósito almejado.

Destaca-se que o operador (LGPD, art. 5º, VII) realiza o tratamento de dados pessoais conforme a LGPD e respeita os critérios estabelecidos pela instituição que exerce o papel de controlador (LGPD, art. 5º, VI), pois essas ações são realizadas concomitantemente pelo GOV.BR (SEPRO), ANAC e pelo DECEA (sob a égide do Destacamento de Controle do Espaço Aéreo e Telemática do Rio de Janeiro (DTCEATM-RJ) e pela Assessoria de Transformação Digital (ATD) do DECEA).

No sistema há a Política de Privacidade que expõe ao usuário os dados que são obtidos para acessar o sistema, além das formas de armazenamento e tratamento, sendo exposto que não há transferências de informações, com exceção aos previstos em Lei (artigo 18 da LGPD).

6 IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

O art. 5º, XVII da LGPD preconiza que o Relatório de Impacto deve descrever “**medidas, salvaguardas e mecanismos de mitigação de risco**”.

Os parâmetros escalares adotados neste documento são apresentados a seguir:

Classificação de risco:

Classificação	Valor
Baixo	5
Moderado	10
Alto	15

Risco enquadrado na região:

- verde, é entendido como baixo;
- amarelo, representa risco moderado; e
- vermelho, indica risco alto.

Detalhamento:

- a) Probabilidade (P): chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19);
- b) Impacto (I): resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18);
- c) Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

Id	Risco Referente ao Tratamento de Dados Pessoais	P	I	Nível de Risco (P X I)
R01	Acesso não autorizado: há o risco de que indivíduos não autorizados acessem o banco de dados, o que poderia levar ao uso indevido de dados pessoais	5	15	75
R02	Violação de dados: há o risco de que os dados pessoais sejam violados, seja por meio de um ataque cibernético ou por falha no sistema de segurança, resultando em perda, roubo ou vazamento de dados pessoais	10	15	150
R03	Decisões automatizadas: o sistema SARPAS NG utiliza algoritmos para analisar os dados pessoais, obtidos via GOV.BR, e gerar informações que podem influenciar decisões automatizadas. Existe o risco de que as decisões tomadas com base nessas informações sejam imprecisas	5	10	50
R04	Uso indevido de dados pessoais: existe o risco de que os dados pessoais coletados pelo sistema sejam usados para fins não autorizados ou não relacionados ao gerenciamento do tráfego aéreo, como comerciais ou de vigilância	5	15	75

Sendo assim, bastará um incidente de segurança supracitados para que o Controlador seja autuado por realizar tratamento não condizente com a expectativas dos titulares destes dados.

7 MEDIDAS PARA TRATAR OS RISCOS

Seguem medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito (LGPD, art. 46).

Risco	Controle/Medida	Efeito sobre o Risco	Risco Residual			Controle/ Medida(s) Aprovados(as)
			P	I	Nível (P x I)	
R01 e R04	Somente usuários autorizados devem ter acesso ao banco de dados. O sistema deve ser projetado de forma a evitar o acesso não autorizado, com a implementação de medidas de segurança, como criptografia e controle de privilégios.	Reduzir	5	10	50	Sim
R02	Segurança de dados: o sistema deve ser projetado de forma a garantir a segurança dos dados pessoais, com a implementação de medidas de segurança, como backup, monitoramento de eventos de segurança, detecção de intrusão e criptografia.	Reduzir	5	5	25	Sim
R03	Risco de decisões automatizadas: a regra de negócio do sistema deve ser periodicamente evoluída para que o algoritmo possa retratar plenamente as necessidades de análise e tratamento dos dados pessoais.	Reduzir	5	5	25	Sim
R04	Transparência e prestação de contas: a coleta, o processamento e o uso de dados pessoais pelo sistema devem ser transparentes para os titulares dos dados por meio de sua política de privacidade.	Reduzir	5	10	50	Sim

Legenda:

Efeito resultante do tratamento do risco com a aplicação do(s) controle(s) descrito(s) na tabela. As seguintes opções podem ser selecionadas: Reduzir, Evitar, Compartilhar e Aceitar. Risco residual é o risco que ainda permanece mesmo após a aplicação de controles para tratar o risco.

Controle/medida aprovado(a) pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

8 APROVAÇÃO

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO Alex Ribeiro Pereira 1º Ten Esp Aer COM SARAM: 3177785 Rio de Janeiro, 08 de julho de 2024	CHEFE DE DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES Marcos Aurélio Valença Belchior CL Eng CMP SARAM: 3038912 Rio de Janeiro, 08 de julho de 2024
ENCARREGADO SETORIAL André Eduardo Jansen Brig Eng SARAM: 2564955 Rio de Janeiro, 08 de julho de 2024	CONTROLADOR SETORIAL Alcides Teixeira Barbacovi Ten Brig Av SARAM: 1213172 Rio de Janeiro, 08 de julho de 2024