

DEPARTAMENTO DE SEGURANÇA PÚBLICA

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

XPTO, 07 de janeiro de 2019

DEPARTAMENTO DE SEGURANÇA PÚBLICA

Histórico de Revisões

Data	Versão	Descrição	Autor
07/01/2019	1.0	Conclusão da primeira versão do relatório	Beltrano Hertz

ATENÇÃO!

<Os trechos marcados em azul neste template são editáveis, notas explicativas ou exemplos, devendo ser substituídos ou excluídos, conforme necessário>.
<Template Versão 1.0 – 25/09/2020>

DEPARTAMENTO DE SEGURANÇA PÚBLICA

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPD

OBJETIVO

O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os 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.

Referência: Art. 5º, XVII da Lei 13.709/2018 (LGPD).

1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador

Departamento de Segurança Pública [IDP*, item 2.1]

Operador

Empresa de Tecnologia e Processamento Fictum [IDP*, item 2.3]

Encarregado

Fulano de Tal [IDP*, item 2.2]

E-mail Encarregado

privacidade@dsp.gov.xp [IDP*, item 2.2]

Telefone Encarregado

+9999 (0) 999 799 9 799
[IDP*, item 2.2]

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

2.1 O Programa de Localização de Desaparecidos realizará tratamentos de dados pessoais de pessoas desaparecidas e dos comunicantes do desaparecimento por meio do Sistema de Localização de Desaparecidos [**EC, itens 1.2 e 1.3].

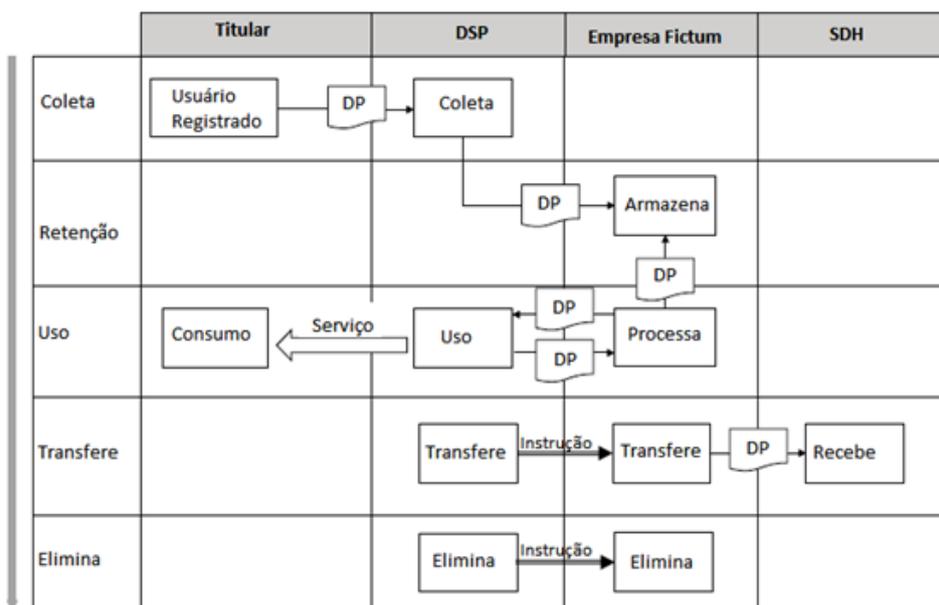
2.2 Dentre o público alvo do Programa também poderão ser tratados dados pessoais de crianças e adolescentes desaparecidos [**EC, itens 1.8.3].

DEPARTAMENTO DE SEGURANÇA PÚBLICA

3 – DESCRIÇÃO DO TRATAMENTO

3.1 – NATUREZA DO TRATAMENTO

3.1.1 Os dados pessoais são coletados mediante preenchimento de formulário eletrônico do Sistema Nacional pelo titular dos dados pessoais. Os dados são transferidos armazenados nas instalações físicas da Empresa de Processamento e Tecnologia Fictum. A empresa Fictum realiza processamento sobre os dados pessoais e disponibiliza para uso do DSP. O DSP disponibiliza os dados pessoais para utilização e consumo do comunicante. O DSP transfere dados de comunicantes e pessoas desaparecidas para a SDH desenvolver as ações de apoio psicológico para as famílias dos desaparecidos. Os dados pessoais podem ser eliminados à pedido do titular. Nesse caso, o DSP encaminha essa solicitação para a empresa Fictum executar a eliminação dos dados pessoais da base de dados do SND [*IDP, item 4.1]. Esse fluxo de tratamento de dados é demonstrado pela figura abaixo [**EC, Anexo, Figura 1].



Legenda figura fluxo de dados:

DP - Dados Pessoais da pessoa desaparecida e do comunicante do desaparecimento.

DSP - Departamento de Segurança Pública representa o controlador dos dados pessoais.

Empresa Fictum - empresa que representa o operador dos dados pessoais.

SDH - Secretaria de Desenvolvimento Humano

Titular - Comunicante do desaparecimento titular dos dados pessoais.

3.1.2 A fonte de dados é o comunicante do desaparecimento mediante o preenchimento de formulário eletrônico do Sistema Nacional de Desaparecidos – SND [*IDP, item 5.2].

3.1.3 São compartilhados com a Secretaria de Desenvolvimento Humano os dados de nome, e-mail, telefone, CPF e endereço residencial do comunicante com o objetivo dessa Secretaria fornecer apoio psicológico para as famílias das pessoas desaparecidas [*IDP, item 11.1].

3.1.4 O operador de dados pessoais é a Empresa de Tecnologia e Processamento Fictum [*IDP, item 2.3], a qual é responsável pela implementação do SND que automatiza todas as operações de

DEPARTAMENTO DE SEGURANÇA PÚBLICA

tratamento de dados pessoais (Coleta, Retenção, Processamento, Compartilhamento e Eliminação) [*IDP, item 3.1].

3.1.5 As medidas de segurança atualmente adotadas são: Controle de Acesso Lógico, Controles Criptográficos, Controles de Segurança em Redes, Proteção Física e do Ambiente [*IDP, itens de 12.1 a 12.3].

3.2 – ESCOPO DO TRATAMENTO

3.2.1 Os dados pessoais tratados pelo PLD abrangem:

- Informações de identificação pessoal: Nome, endereço residencial e telefone da vítima; e Endereço, Cidade e UF do desaparecimento; e Nome, e-mail, telefone e endereço residencial do comunicante; [*IDP, item 7.1.1]
- Informações de identificação atribuídas por instituições governamentais: CPF, RG e órgão expedidor do RG da vítima; e CPF do comunicante; [*IDP, item 7.1.2]
- Dados de identificação eletrônica: Endereço IP do dispositivo eletrônico do comunicante; [*IDP, item 7.1.3]
- Detalhes pessoais: Data de nascimento e sexo da vítima; [*IDP, item 7.3.1]
- Descrição Física: Cor dos olhos, altura, sinais particulares (ex. tatuagem) e cabelo da vítima; [*IDP, item 7.3.4]
- Familiares ou membros da família (Composição Familiar): Nome de pai e mãe da vítima; [*IDP, item 7.6.3]
- Vídeo e imagem: Foto da vítima; [*IDP, item 7.14.1]
- Registro boletim de ocorrência: Número do boletim de ocorrência, data do fato, Delegacia de registro e Data do registro da ocorrência; [*IDP, item 7.15.1]
- Desaparecimento (Boletim de Ocorrência): Circunstâncias do desaparecimento; e [*IDP, item 7.15.2]
- Dado sensível que revela origem racial ou étnica: Cor da pele da vítima. [*IDP, 8.1]

3.2.2 A quantidade de dados pessoais tratados são de 29 dados pessoais e 1 dado pessoal sensível (cor da pele) [*IDP, 9.2]. A frequência de tratamento dos dados pessoais é 24x7 (24 horas por dia nos 7 dias da semana) para comunicação dos desaparecimentos e as demais fases e operações de tratamento são realizadas no horário comercial em dias úteis [*IDP, 9.1].

3.2.3 Os dados pessoais obtidos serão mantidos armazenados durante a existência do Programa de Localização dos Desaparecidos [*IDP, itens das seções 7 e 8]. Esse período de armazenamento poderá ser revisto em alinhamento a qualquer nova disposição legal sobre prazo de retenção [**EC, item 2.5].

3.2.4 O número de titulares afetados pelo tratamento é de 950.000 [**EC, item 2.3] entre comunicantes e vítimas desaparecidas, atingindo volume de 1GB de dados pessoais [**EC, item 2.3].

3.2.5 A abrangência do tratamento de dados pessoais é nacional [*IDP, 5.1] para manutenção do cadastro nacional de desaparecidos e atuação das equipes do Programa de Localização dos Desaparecidos - PLD distribuídas por todos os estados do país [**EC, item 1.3].

DEPARTAMENTO DE SEGURANÇA PÚBLICA

3.3 – CONTEXTO DO TRATAMENTO

3.3.1 A natureza do relacionamento dos indivíduos com o DSP no âmbito do PLD é centrada na pessoa do comunicante do desaparecimento, o qual é responsável por informar dados da pessoa desaparecida, do boletim de ocorrência e dele próprio [**EC, item 1.3].

3.3.2 Qualquer atualização, compartilhamento dos dados pessoais ou acessos suspeitos ao SND são avisados ao titular [**EC, item 1.8.1]. Embora o campo CPF e nome do comunicante seja restrito para alteração e o campo e-mail exija um procedimento especial de atualização, os demais dados pessoais podem ser acessados e atualizados permanentemente pelo titular dos dados em questão. O titular pode requisitar informações sobre seus dados pessoais a qualquer momento [**EC, item 1.8.2].

3.3.3 Poderão ser tratados dados pessoais de crianças e adolescentes desaparecidos [*IDP, item 10.3].

3.3.4 O tratamento de dados é realizado de acordo com a expectativa do titular de dados, conforme aviso de privacidade de ciência do titular dos dados ao se cadastrar no SND. Existem casos em que os titulares de dados (comunicantes) tornam públicos os dados da comunicação de desaparecimento (exceto CPF, RG e Endereço IP) na esperança de que isso acelere a localização da pessoa desaparecida [**EC, item 1.8.4].

3.3.5 O DSP detém razoável experiência em tratamento de dados pessoais e tem estabelecido ações para implementação (conformidade) do previsto pela LGPD [**EC, item 1.8.5].

3.3.6 O DSP utiliza recursos de segurança robustos e pretende investir em novas aplicações para 2020 [**EC, item 1.8.6].

3.4 – FINALIDADE DO TRATAMENTO

3.4.1 Promover ações de identificação e busca de pessoas desaparecidas, bem como facilitar o apoio psicológico às famílias dos desaparecidos [*IDP, item .6.2].

3.4.2 Os resultados pretendidos para os titulares de dados pessoais são: apoio psicológico para as famílias das pessoas desaparecidas; e promoção do respeito pela dignidade das famílias e das pessoas desaparecidas [*IDP, item .6.4].

3.4.3 Os benefícios esperados para o órgão, entidade ou para a sociedade como um todo são: dados consolidados, centralizados e atualizados relativos ao número de pessoas desaparecidas no País; e informações qualificadas para o estabelecimento de ações coordenadas por equipe de localização de desaparecidos com abrangência nacional a fim de reduzir o número de pessoas desaparecidas [*IDP, item .6.5].

4 – PARTES INTERESSADAS CONSULTADAS

4.1 Analistas de segurança da informação do DSP e da Empresa de Tecnologia e Processamento Fictum, os quais indicaram as oportunidades de melhoria para aperfeiçoamento da proteção dos dados pessoais tratados [**EC, item 6.1.1].

4.2 Consultor jurídico DSP, responsável por emitir parecer sobre a conformidade do tratamento de dados do PLD em relação aos aspectos legais da LGPD [**EC, item 6.1.2].

4.3 Coordenadores, servidores e Diretores do DSP e da Secretaria de Desenvolvimento Humano a fim de obter informações técnicas e administrativas sobre o processo de trabalho executado no

DEPARTAMENTO DE SEGURANÇA PÚBLICA

âmbito do PLD [****EC**, item 6.1.3].

4.4 Encarregado do tratamento de dados pessoais, que desempenhou o papel de conduzir o levantamento e apreciar as informações técnicas, administrativas, legais e de riscos fornecidas pelas demais partes consultadas [****EC**, item 6.1.4].

4.5 Famílias das pessoas desaparecidas (comunicantes do desaparecimento), não foram consultadas mediante pesquisa, elas expressaram sua opinião em passeatas e manifestações públicas, solicitando das autoridades uma ação articulada para localização das pessoas desaparecidas [****EC**, item 6.1.5].

4.6 Com exceção dos comunicantes de desaparecimento, todas as demais partes consultadas participaram do processo de análise de riscos relativos ao tratamento dos dados pessoais [****EC**, item 6.2].

5 – NECESSIDADE E PROPORCIONALIDADE

5.1 – FUNDAMENTAÇÃO LEGAL

5.1.1 A hipótese legal para tratamento de dados pessoais é o art. 7º, III da LGPD: “pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres (...)” [***IDP**, item 6.1].

5.1.2 A necessidade de tratamento é respaldada pela previsão legal constante do Decreto 8.956/2018, que institui o PLD [***IDP**, item 6.3].

5.2 – QUALIDADE E MINIMIZAÇÃO DOS DADOS

5.1.1 A escolha dos dados coletados para implementação do PLD foi resultado de intensos estudos realizados pelo DSP com a preocupação de coletar o mínimo de dados necessários para execução da política pública relacionada com esse Programa. As informações sobre pessoas desaparecidas utilizadas no PLD são providas pelo comunicante (fonte de informação). Ao acessar o SND pela primeira vez, ele manifesta sua concordância a Política de Privacidade do PLD, a qual em seu conteúdo destaca a responsabilidade do comunicante em informar dados precisos e atualizar qualquer mudança nos dados informados, como por exemplo, mudança de endereço, telefone ou e-mail de contato [****EC**, item 7.1].

5.1.2 Está previsto para o próximo ano a integração do SND com bases de outros órgãos e entidades com o objetivo de assegurar a qualidade e atualização dos dados pessoais [****EC**, item 7.2].

5.3 – MEDIDAS PARA ASSEGURAR CONFORMIDADE DO OPERADOR

5.3.1 Em períodos planejados, o DSP conduz inspeção sobre os processos de tratamento de dados executados pela Empresa de Tecnologia e Processamento Fictum a fim de avaliar se esses processos estão em conformidade com as diretrizes definidas pelo controlador [****EC**, item 7.4].

5.4 – MEDIDAS PARA ASSEGURAR DIREITOS DO TITULAR DOS DADOS

5.4.1 O Sistema de Informação ao Cidadão (e-SIC.XP) e a Ouvidoria (Fala.XP) são disponibilizados para que os titulares dos dados pessoais possam demandar as solicitações previstas pelo art. 18º da LGPD. A Política de Privacidade informa sobre o direito que o titular dos dados pessoais tem de realizar qualquer uma das referidas solicitações. A Política de Privacidade pode ser encontrada no

DEPARTAMENTO DE SEGURANÇA PÚBLICA

link <https://www.dsp.gov.xp/publicacoes/politica-privacidade>. Caso o usuário identifique alguma falha ou vulnerabilidade de segurança no sistema, é possível reportá-la também pela Ouvidoria (Fala.XP) [****EC**, item 7.5].

5.4.2 Quando solicitado pelo titular do dado pessoal, o DSP fornecerá informações de privacidade (confirmação de existência ou o acesso a dados pessoais) por meio de e-mail ou sob forma impressa, de acordo com a solicitação do referido titular [****EC**, item 7.6].

5.5 – SALVAGUARDAS PARA AS TRANSFERÊNCIAS INTERNACIONAIS DE DADOS

5.5.1 O PLD não realiza qualquer tipo de transferência internacional de dados [***IDP**, item 13.1].

6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Id	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)
R01	Acesso não autorizado.	10	15	150
R02	Coleção excessiva.	10	15	150
R03	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	10	15	150
R04	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	10	15	150
R05	Falha/erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com dado equivocado, ausência de validação dos dados de entrada, etc.).	10	15	150
R06	Informação insuficiente sobre a finalidade do tratamento.	15	15	225
R07	Modificação não autorizada.	10	15	150
R08	Perda.	15	15	225
R09	Reidentificação de dados pseudonimizados.	15	15	225
R10	Remoção não autorizada.	10	15	150
R11	Retenção prolongada de dados pessoais sem necessidade.	15	15	225
R12	Roubo.	10	15	150
R13	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	15	150
R14	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	10	15	150

DEPARTAMENTO DE SEGURANÇA PÚBLICA

7 – MEDIDAS PARA TRATAR OS RISCOS

Risco	Medida(s)	Efeito sobre o Risco ¹	Risco Residual ²			Medida(s) ³ Aprovada(s)
			P	I	Nível (P x I)	
R01 Acesso não autorizado.	Responsabilização: Compliance com a Privacidade; Gestão de Mudanças:	Reduzir	5	10	50	Sim

Legenda:

¹ Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: Reduzir, Evitar, Compartilhar e Aceitar.

² Risco residual é o risco que ainda permanece mesmo após a aplicação de medidas para tratar o risco.

³ Medida aprovada pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

DEPARTAMENTO DE SEGURANÇA PÚBLICA

8 – APROVAÇÃO

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO	ENCARREGADO
[**EC, Seção 8] <hr/> Beltrano Hertz Matrícula/SIAPE: XP120-1 XPTO, 07 de janeiro de 2019	[**EC, Seção 8] <hr/> Fulano de Tal Matrícula/SIAPE: XP185-3 XPTO, 07 de janeiro de 2019
AUTORIDADE REPRESENTANTE DO CONTROLADOR	AUTORIDADE REPRESENTANTE DO OPERADOR
[**EC, Seção 8] <hr/> Ciclano Watts Matrícula/SIAPE: XP14-2 XPTO, 07 de janeiro de 2019	[**EC, Seção 8] <hr/> Joules Volts Matrícula/SIAPE: F4525-1 XPTO, 07 de janeiro de 2019

Legenda:

* Informação obtida da guia “PLD” do Inventário de Dados Pessoais (IDP). Veja o template do Estudo de Caso da Oficina de Inventário de Dados Pessoais disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/templateinventariodadospessoais_estudo-caso_v1.xlsx>

** Informação obtida diretamente do Estudo de Caso (EC) do RIPD disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/estudo-de-caso_pld_oficina-ripd_v1.pdf>