Despacho Ministerial

Inquérito Civil Público n. *08190.005366/18-16* **Vivo Ads**

O **Ministério Público do Distrito Federal e Territórios**, por sua **Unidade Especial de Proteção de Dados e Inteligência Artificial**, requisita à **Telefônica Brasil S.A.** (**Vivo**) que elabore Relatório de Impacto à Proteção de Dados Pessoais (*Data Protection Impact Assessment – DPIA*), no prazo de 60 (sessenta) dias, em relação ao tratamento dos dados usados para o produto Mídia Geolocalizada do serviço **Vivo Ads**.

O Relatório de Impacto à Proteção de Dados Pessoais deverá conter os seguintes tópicos:

1 – Como a organização descreve o tratamento de dados realizado

A natureza do tratamento é o que a organização planeja fazer com os dados pessoais. Isso deve incluir:

Como a organização coleta os dados;

Como a organização armazena os dados;

Como a organização usa os dados;

Quem tem acesso aos dados;

Com quem são compartilhados os dados;

Se a organização utiliza operadores (pessoa natural ou jurídica que realiza o tratamento de dados em nome do operador) para tratar os dados;

Períodos de retenção;

Medidas de segurança;

Se a organização utiliza novas tecnologias, e;

Se a organização usa algum tipo novo de tratamento.

O escopo é o que o tratamento abrange. Isso deve incluir:

A natureza dos dados pessoais;

O volume e a variedade dos dados pessoais;

A sensibilidade dos dados pessoais;

A extensão e frequência do tratamento;

A duração do tratamento;

O número de dados envolvidos, e;

A área geográfica coberta.

O contexto do tratamento é um quadro mais amplo, incluindo fatores internos e externos que podem afetar as expectativas ou o impacto. Isso deve incluir:

A fonte dos dados;

A natureza do relacionamento da organização com os indivíduos;

Até que ponto os indivíduos têm controle sobre seus dados;

Até onde os indivíduos provavelmente esperam o tratamento;

Se entre os indivíduos incluem-se menores de 18 anos ou outras pessoas vulneráveis;

Qualquer experiência anterior com este tipo de tratamento;

Quaisquer avanços relevantes em tecnologia ou segurança, e;

Quaisquer questões atuais de interesse público.

O objetivo do tratamento é o motivo pelo qual a organização faz o tratamento dos dados. Isso deve incluir:

Seus interesses legítimos, quando relevantes;

O resultado pretendido para os indivíduos;

Os benefícios esperados para a organização ou para a sociedade como um todo.

2 – Como a organização avalia a necessidade e proporcionalidade do tratamento de dados

Existe alguma outra maneira razoável de alcançar o mesmo resultado;

Qual a base legal usada para o tratamento de dados;

Como a organização pretende garantir a qualidade dos dados;

Como a organização pretende fornecer informações de privacidade para os indivíduos;

Medidas adotadas para garantir o cumprimento da legislação e das ordens dadas aos operadores, e;

Quais são as salvaguardas para as transferências internacionais de dados.

3 – Como a organização identifica e avalia os riscos

Deve ser considerado o impacto potencial sobre os indivíduos e qualquer dano que seu tratamento possa causar, seja físico, emocional ou material. Em particular, observe se o tratamento poderá contribuir para:

Incapacidade de exercer direitos (incluindo, mas não se limitando, a direitos de privacidade);

Incapacidade de acessar serviços ou oportunidades;

Perda de controle sobre o uso de dados pessoais;

Discriminação;

Roubo de identidade ou fraude;

Perda financeira;

Danos à reputação;

Danos físicos;

Perda de confidencialidade, ou;

Qualquer outra desvantagem econômica ou social significativa.

A organização deve incluir uma avaliação dos riscos de segurança, incluindo fontes de risco e o impacto potencial de cada tipo de violação (incluindo acesso ilegítimo, modificação ou perda de dados pessoais).

Para avaliar se o risco é alto, a organização precisa considerar tanto a probabilidade quanto a gravidade do possível dano. O dano não precisa ser inevitável para se qualificar como risco. Qualquer possibilidade significativa de danos muito sérios pode ser suficiente para se qualificar como alto risco. A organização deve se atentar para o fato de que uma alta probabilidade de danos generalizados, ainda que com impactos menores, pode ser igualmente considerada de alto risco.

A organização deve fazer uma avaliação objetiva dos riscos. É útil usar uma matriz estruturada para pensar sobre a probabilidade e a gravidade dos riscos:

Severity of impact				
	Serious harm	**Low risk**	**High risk**	**High risk**
	Some impact	**Low risk**	**Medium risk**	**High risk**
	Minimal impact	**Low risk**	**Low risk**	**Low risk**
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

4 – Como a organização identifica e mitiga os riscos

Contra cada risco identificado, registre a fonte. A organização deve considerar opções para reduzir estes riscos, como por exemplo:

Decidir não coletar certos tipos de dados;

Reduzir o escopo do processamento;

Reduzir os períodos de retenção;

Tomar medidas adicionais de segurança tecnológica;

Treinar os colaboradores para garantir que os riscos sejam antecipados e gerenciados;

Anonimizar ou pseudoanonimizar os dados, sempre que possível;

Elaborar orientações ou processos internos para evitar riscos;

Colocar em prática acordos claros de compartilhamento de dados;

Fazer alterações nas políticas de privacidade;

Implementar novos sistemas para ajudar os indivíduos a exercerem seus direitos.

5 – Conclusão do Relatório de Impacto à Proteção de Dados Pessoais

A Organização deve informar:

Que medidas adicionais pretende adotar;

Se cada risco foi eliminado, reduzido ou aceito;

O nível global de risco residual, após a adoção de medidas adicionais.

6 – Assinaturas dos Responsáveis pela Elaboração do Relatório de Impacto à Proteção de Dados Pessoais (Encarregado/ *Data Protection Officer – DPO* ou Diretor da Organização)

Brasília-DF, 16 de abril de 2019.

Frederico Meinberg Ceroy
Promotor de Justiça
Coordenador da ESPEC