ROTEIRO PARA ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

1. O que é o inventário de dados:

O Inventário de Dados Pessoais representa o documento primordial para documentar o tratamento de dados pessoais realizados pela instituição, conforme estabelece o art. 37 da Lei nº 13.709, de 14 de agosto de 2018 (LGPD). Consiste em uma avaliação do que os órgãos e entidades fazem com os dados pessoais, identificando quais dados pessoais são tratados, onde estão e que operações são realizadas com eles. Portanto, é um diagnóstico o mais completo e realista possível sobre todos os tratamentos de dados pessoais realizados pela instituição, sendo um documento vivo e de atualização permanente, sendo recomendável atualizar sempre que necessário, mas, pelo menos, 1 (uma) vez a cada 12 meses. Além disso, o IDP é um documento importante para subsidiar a avaliação de impacto à proteção de dados pessoais com vistas a verificar a conformidade da instituição no que se refere ao preconizado pela LGPD.

2. O que deve constar do registro mantido pelo inventário de dados pessoais?

Em regra, o registro envolve descrever informações em relação ao tratamento de dados pessoais realizado pelo órgão ou entidade como:

- atores envolvidos (agentes de tratamento e o encarregado);
- finalidade (o que a instituição faz com o dado pessoal);
- hipótese (arts. 7º e 11 da LGPD);
- previsão legal;
- dados pessoais tratados pela instituição;
- categoria dos titulares dos dados pessoais;
- tempo de retenção dos dados pessoais;
- instituições com as quais os dados pessoais são compartilhados;
- transferência internacional de dados (art. 33 LGPD); e
- medidas de segurança atualmente adotadas.

3. Como elaborar o inventário de dados pessoais?

De acordo com o artigo 37 da LGPD, cabe ao controlador e ao operador manterem os registros das operações de tratamento de dados pessoais que realizam. Dessa forma, segue sugestão para auxiliar os órgãos e entidades, que exercem papel de controlador de dados pessoais, na elaboração de inventário de dados pessoais. Lembrando que o modelo sugerido pode ser adaptado para se adequar a cada contexto em particular.

3.1 – identificação do processo/serviço:

Analisar os dados pessoais por serviço e/ou processo de negócio realizado pelo órgão ou entidade. Ressalta-se que mesmo os dados pessoais dos serviços e/ou processo não digitais, devem ser inventariados. Sugere-se colocar aqui a data da criação do inventario, bem como a data da última atualização.

3.2 – finalidade do processo de tratamento de dados pessoais:

Identificar a finalidade específica do tratamento de dados pessoais, de acordo com o art. 6º, I, da LGPD.

3.3 – atores envolvidos:

Identificar as pessoas envolvidas no tratamento de dados pessoais.

3.4 – dados pessoais utilizados:

Identificar quais os dados pessoais são tratados no serviço, processo ou política pública, Inventariar os dados pessoais utilizados pela instituição possibilitará avaliar se todos os dados pessoais usados são realmente necessários e adequados para realização de suas finalidades (LGPD, art. 6º, III).

3.5 – dados pessoais sensíveis utilizados:

Identificar quais os dados pessoais sensíveis são tratados no serviço, processo ou política pública, conforme art 5º, II, da LGPD. Realizar o inventário de dados pessoais sensíveis é extremamente importante, visto que o uso indevido desses dados podem resultar em algum tipo de discriminação em relação ao titular dos dados pessoais sensíveis.

3.6 – categoria dos titulares de dados

Definir quais os titulares dos dados pessoais tratados, tais como cidadãos, servidores públicos, partes contratadas, beneficiários de uma política pública, candidatos a um concurso público, entre outros.

3.7 – origem dos dados

Informar de que forma os dados pessoais ou dados pessoais sensíveis são inicialmente coletados ou inseridos no serviço, processo de negócio ou política pública.

3.8 – localização e armazenamento

Informar em que local os dados são armazenados e, se possível, quem possui acesso a eles.

3.9 – base legal de tratamento

Informar qual das bases legais de tratamento constantes da LGPD (art. 7, 11 e 14, da LGPD).

3.10 – previsão legal

Informar quais as previsões legais existentes para regulamentar a realização daquele serviço, processo ou política pública.

3.11 – ciclo de vida dos dados

Definir qual o tempo de vida dos dados pessoais, incluindo desde o momento da sua coleta ou criação até o momento da sua extinção.

3.12 – compartilhamento com terceiros

Definir os compartilhamentos dos dados pessoais feitos com terceiros externos à execução do serviço, processo de negócio ou política pública. Ou seja, Informar com quais instituições os dados pessoais são compartilhados e para qual finalidade.

3.13 – transferência internacional de dados

Esta fase do IDP envolve destacar as organizações internacionais que recebem dados pessoais por meio de qualquer tipo de transferência ou meio compartilhamento

3.14 – sistemas, aplicações ou banco de dados utilizados

Definir sistemas, aplicações digitais ou bancos de dados utilizados em quaisquer das etapas de tratamento de dados pessoais do serviço, processo de negócio ou política pública.

3.15 – medidas de segurança da informação

Esta fase envolve identificar as atuais medidas de segurança, técnicas administrativas implementadas e a descrição dos controles que visam assegurar a integridade dos dados pessoais, minimizando os riscos como, por exemplo, de perda ou vazamento de dados.

3.16 – anonimização ou criptografia

Descrever se há alguma técnica de anonimização ou criptografia realizada sobre os dados pessoais tratados.

3.17 – contratos, convênios, termos de cooperação e demais documentos congêneres que formalizam compartilhamento

Informar contratos, convênios, termos de cooperação, acordos de resultado e demais documentos jurídicos congêneres que formalizam o compartilhamento de dados com terceiros

3.18 – termos de uso e política de privacidade vigentes

Informar se existem termo(s) de uso e política de privacidade vigentes e disponíveis publicamente para o titular de dados pessoais