Procedimento de Privacy By Design

1 Introdução

Este documento estabelece os princípios e diretrizes básicos para garantir que o futuro da privacidade seja assegurado em SUAPE. Deste modo, o objetivo não é apenas estabelecer uma estrutura regulatória para garantir a privacidade, mas também novas medidas de criação que levam em consideração a privacidade desde o início do desenvolvimento do produto, aliado ao conceito do *Privacy By Design*.

O *Privacy By Design* é caracterizado pela abordagem proativa, de modo que incentiva a antecipação da proteção da privacidade contra os efeitos negativos e invasivos por meio do que será criado. Portanto, há o efeito preventivo.

O objetivo deste documento é registrar que a proteção da privacidade deve abranger não apenas medidas reativas, mas as medidas preventivas. Sendo assim, a técnica da privacidade desde a concepção é adequada a qualquer organização que irá iniciar um novo produto, ou processo de negócio que envolva dados pessoais, para garantir e resguardar que a segurança da informação e a privacidade dos dados estejam presentes em todas as fases desde a criação ao lançamento.

Para ser eficaz, o Privacy by Design precisa ser parte integrante do processo de criação (desde à concepção), de modo que possibilite a identificação dos efeitos potenciais que os processos propostos podem causar sobre a privacidade dos dados, além de identificar como os possíveis efeitos prejudiciais à privacidade, podem ser mitigados.

2 Guideline para Privacy By Design

2.1 Escopo e Requisitos do Privacy By Design

A aplicação do Privacy By Design, é possível delimitar 5 etapas principais no projeto.

- **1ª Iniciação da aplicação:** A aplicação da técnica deve ser realizada no estágio inicial, realizando uma Avaliação Preliminar de Impacto de Privacidade. Utilize o Questionário para Privacy By Design, para desenvolver a avaliação preliminar.
- **2ª Análise de Fluxo de Dados:** Esta etapa é destinada à análise dos fluxos de dados pessoais dentro do que está sendo analisado.

- **3ª Análise da Privacidade:** A análise de privacidade examina os fluxos de dados no contexto das políticas, procedimentos e legislação vigente sobre a privacidade e proteção de dados aplicáveis. Utilize o Questionário para Privacy By Design para coletar informações relevantes sobre os fluxos de dados pessoais, e depois lance-os na ferramenta para Privacy By Design para efetuar análise da privacidade.

- **4ª Relatório de Análise de Impacto de Privacidade:** Esta fase analisa e processa os resultados das etapas anteriores. O objetivo desta fase é documentar os riscos de privacidade e proteção de dados, juntamente com uma discussão de estratégias para eliminação ou mitigação desses riscos.

- **5ª Registro de Relatórios Privacy By Design:** Após a finalização integral de todas as etapas, registre na planilha de registro de Relatórios do Privacy By Design, para ter um controle de todos os relatórios elaborados.

2.2 Calendários e Programação

Este procedimento pode ser iniciado a qualquer momento quando houver a necessidade de iniciar a análise de um novo serviço ou processo de negócio que necessite do privacy by design.

2.3 Análise de Fluxo de Dados

Após a realização da avaliação preliminar, é necessário mapear todo o fluxo de dados pessoais, separando-os por agrupamentos de categorias, ou por setores à depender do que está sendo analisado.

Esta análise deve abranger desde a coleta de dados, até o seu uso e divulgação.

Utilize como aliado à execução desta etapa o *Questionário para Privacy By Design*, e a *Ferramenta de Privacy By Design.*

2.4 Análise da Privacidade

Esta etapa abrange a explicação de como as exigências legais são atendidas ou por que não é atendido diante a análise de fluxos de dados realizada no tópico anterior. Para analisar a privacidade, se baseie nos princípios da

LGPD, verificando a devida adequação da coleta e tratamento de dados de acordo com as bases legais de tratamento, finalidade do tratamento, bem como o interesse legítimo para a realização do tratamento.

Para a execução desta parte, é necessário verificar a adequação da coleta e tratamento com os requisitos universais da privacidade, e da Lei Geral de Proteção de Dados, para chegar à conclusão se a privacidade está sendo cumprida ou não.

O relatório não deve se limitar a questões de *compliance* e deve discutir e analisar a proposta com relação às potenciais vantagens e riscos em termos de privacidade da informação e identificar as melhores práticas quando possível.

Utilize como aliado à execução desta etapa o *Questionário para Privacy By Design*, e a *Ferramenta de Privacy By Design.*

2.4.1 Identificação de Riscos

Identifique como o fluxo de dados podem impactar nos direitos e liberdades do titular. O processo de identificação dos riscos aos direitos e liberdades dos titulares dos dados em razão da nossa coleta e tratamento, consistirá na avaliação da probabilidade e impacto, conforme as etapas a seguir:

2.4.1.1 Avaliação da Probabilidade

Para avaliar a probabilidade, é necessário avaliar os cenários de riscos e pensar em todas as possibilidades de que podem levar a ocorrência de problemas e impactos, uma vez que a privacidade está sendo analisada antes de instituir de fato a coleta de dados. Além disso, para avaliar a probabilidade é possível realizar pesquisas sobre casos semelhantes.

A probabilidade de cada risco é classificada em uma escala numérica de 1 (baixa) a 5 (alta). A orientação geral para o significado de cada grau é dada na *Tabela 1*. Ao avaliar a probabilidade de um risco, os controles existentes devem ser levados em consideração.

Grau	Descrição	Resumo
1	Improvável	Nunca aconteceu antes e não há razões para acreditar que pode acontecer agora
2	Improvável	Existe a possibilidade de que isso aconteça, mas provavelmente não
3	Provável	O risco é mais provável de acontecer do que não

4	Muito provável	Muito difícil não acontecer com base em situações anteriores ou nas circunstâncias atuais
5	Quase certo	Ou acontece regularmente ou há alguma razão para acreditar que é praticamente iminente

Tabela 1 – Orientação de probabilidade de risco

2.4.1.2 Avaliação de Impacto

Esta avaliação define a estimativa do impacto que o risco poderia causar, sobre os direitos e liberdades do titular, deve ser mensurado, levando em conta os controles já existentes na organização que diminuem o impacto, desde que sejam eficazes.

Deve-se considerar o impacto nos seguintes fatores:

- Financeiro
- Saúde e segurança
- Reputação
- Obrigações legais, contratuais ou regulamentares
- Outros impactos potenciais

O impacto de cada risco deve ser classificado em uma escala numérica de 1 (baixa) a 5 (alta).

2.5 Ações de Correção

Ao analisar os riscos através do impacto e da probabilidade, aqueles que extrapolarem o limite da razoabilidade para SUAPE deverão ser corrigidos.

Apesar de nem sempre ser possível realizar a correção integral do risco, a organização tem a prerrogativa de aceitar, modificar, evitar ou compartilhar esses riscos.

2.6 Relatório de Análise de Impacto de Privacidade

Finalizando todas as análises das etapas anteriores, é necessário a elaboração do relatório de Análise de Impacto na Privacidade, de acordo com os resultados obtidos, indicando as ações necessárias para garantir a privacidade e segurança dos dados pessoais.

Utilize o *Relatório de Privacy By Design* para a elaboração do relatório, e armazene-o em local seguro como forma de evidenciar que de fato houve a aplicação do *Privacy By Design*.

2.7 Registre o Relatório

Após a elaboração do relatório, registre-os na planilha de registro de relatórios do *Privacy By Design*, para deixar evidenciado todos os relatórios