ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

1. Tema

Produção e Qualidade

2. Subtema

Gestão da Qualidade

3. Categoria de serviço

Acesso a Serviços de Terceiros

4. Tipo de serviço / instrumento

Consultoria tecnológica / Acesso a Serviço Tecnológico

5. Modalidade

Presencial e/ou a distância

6. Público alvo

ME, EPP, MEI, Produtor Rural e Artesão

7. Setor indicado

Agronegócio, Comércio, Indústria e Serviços

8. Macrossegmento

-

9. Descrição

ETAPA 01 | PREPARAÇÃO

Analisar os requisitos de PD&P e seus impactos sobre o negócio; identificar leis, regulamentos e normas relevantes.

1. Estabelecer e organizar a governança de PD&P

1.1. Estabelecer os marcos críticos a serem atingidos pelo programa de Governança em Privacidade

1.2. Incluir a lista de contatos dos Encarregados de eventuais fornecedores e parceiros comerciais do negócio

2. Identificar leis pertinentes sobre o tema

2.1. Levantar normas (leis, portarias, resoluções, etc.) e manifestações (guias, estudos, notas técnicas, pareceres) da Autoridade Nacional de Proteção de Dados (ANPD) sobre o tema

3. Gerenciar o envolvimento da alta administração e das partes interessadas

3.1. Estabelecer calendário de reuniões periódicas com partes interessadas

4. Estabelecer o processo de conscientização e treinamentos

4.1. Criar Plano de Treinamento para colaboradores anual

4.2. Reunir, se aplicável, com unidades internas responsáveis pelos setores de comunicação/marketing e recursos humanos, para elaborar Plano de Comunicação e Conscientização

ENTREGAS ETAPA 01:

- Programa de Governança em Privacidade;
- Relação de Encarregados de eventuais fornecedores e parceiros;
- Inventário de normas e guias pertinentes sobre o tema de PD&P;
- Calendário de reuniões periódicas;
- Plano de Treinamento para colaboradores;
- Plano de Comunicação e Conscientização em PD&P.

ETAPA 02 | ORGANIZAÇÃO

Estabelecer as estruturas organizacionais e os mecanismos necessários ao atendimento das necessidades de conformidade com a legislação de proteção de dados pessoais

1. Manter e fortalecer o Programa de Governança, as Políticas Internas e os Controles de Governança em PD&P

1.1. Avaliar a necessidade de atualizar ou criar políticas, normas e procedimentos internos para assegurar a conformidade com a proteção de dados pessoais e privacidade

2. Atribuir e manter as responsabilidades em relação à PD&P

2.1. Revisitar, se aplicável, cada um dos riscos identificados no ciclo anterior de execução do DPMS

2.2. Agendar reunião com cada unidade que contém riscos envolvidos para propor medidas de adequação

3. Manter o comprometimento institucional com relação à PD&P
   3.1. Levantar documentos internos relevantes, relacionados ao tema, que devam ser publicados internamente (intranet, se for o caso)
   3.2. Reunir com stakeholders para apresentação e esclarecimentos sobre documentos relevantes
   3.3. Assegurar que todos os colaboradores tenham conhecimento adequado sobre políticas internas, principais procedimentos e normas de segurança relacionadas ao tratamento
4. Implementar e operar sistemas automatizados de PD&P
   4.1. Configuração do formulário de registro das atividades de tratamento (RoPA)
   4.2. Incluir os processos mapeados por meio de planilhas
   4.3. Configurar a pesquisa de *due dilligence* com os fornecedores
5. Desenvolver planos de ação para implementação
   5.1. Após a aprovação das medidas de prevenção e mitigação, estabelecer plano de ação para implementação dessas medidas

ENTREGAS ETAPA 02:

- Revisão das políticas, normas e procedimentos;
- Aprovação das medidas de prevenção e mitigação de riscos identificados junto às áreas de negócio;
- Disseminação e socialização de documentos relevantes relacionados ao tema de PD&P;
- Plano de ação para implementação das medidas de mitigação de riscos.

ETAPA 03 | IMPLEMENTAÇÃO

Realizar as atividades estabelecidas no plano de ação; registrar as operações de tratamento de dados pessoais; desenvolver as atividades constantes do Plano de Treinamento e Conscientização; criar canal de atendimento às solicitações dos titulares

1. Executar atividades de integração de PD&P
   1.1. Incluir notificação sobre cookies nas aplicações web
   1.2. Fazer inventário dos bancos de dados administrados
   1.3. Fazer inventário dos diretórios de arquivos (file server)

1.4. Levantar quais outros diretórios devem ter seus documentos digitais mapeados

2. Registro de todas as operações que envolvam dados pessoais
   2.1. Reunião com cada responsável pelos processos de negócio para preenchimento do formulário digital de RoPA
3. Automatizar as requisições dos titulares de dados pessoais
4. Implementar controles de segurança de dados pessoais
   4.1. Elaborar/revisar política de backup
   4.2. Elaborar relatório periódico de teste de integridade de backup
   4.3. Acompanhar a ativação dos serviços de cibersegurança
   4.4. Manter registro de todos os incidentes envolvendo dados pessoais

ENTREGAS ETAPA 03:

- Mapeamento dos dados estruturados e não estruturados;
- Registros das atividades de tratamento (RoPA);
- Automatização de processos de atendimento aos titulares;
- Integridade dos backups;
- Configurar central de registro de incidentes.

ETAPA 04 | GOVERNANÇA

Reunir informações sobre as atividades realizadas, mediante a elaboração dos seguintes relatórios: (i) treinamento e conscientização; (ii) impacto à proteção de dados e (iii) listagem de documentos elaborados (políticas, normas e procedimentos internos)

1. Implementar práticas para gerenciar o tratamento de dados pessoais
   1.1. Levantar informações sobre treinamentos e campanhas de conscientização de proteção de dados e de segurança da informação
2. Avaliar riscos relacionados à proteção de dados pessoais
   2.1. Elaborar relatório de riscos relacionados à proteção de dados pessoais com a respectiva relação das medidas técnicas e administrativas necessárias para tratá-los/mitigá-los
   2.2. Avaliar os riscos residuais e apresentá-los às instâncias decisórias competentes
   2.3. Elaborar relatórios de impacto à proteção de dados (RIPDs) referentes a dados críticos e sensíveis
3. Manter documentação atualizada
   3.1. Propor atualizações no relatório de lições aprendidas, se aplicável

ENTREGAS ETAPA 04:

- Relatório sobre treinamentos institucionais e campanhas de conscientização executadas;
- Relatório a respeito de riscos relacionados a dados pessoais para subsidiar a estratégia de compliance;
- Relatórios de impacto à proteção de dados (RIPDs);
- Relatório de lições aprendidas.

ETAPA 05 | ANÁLISE E MELHORIA

Avaliar e melhorar todos os aspectos específicos do Programa de Conformidade em LGPD, com a elaboração de relatório de lições aprendidas e com a atualização do Plano de Ação, para que sejam definidos os próximos passos para a adequação

1. Monitorar leis e regulamentos
   1.1. Analisar cada nova lei e regulamento relacionados à proteção de dados pessoais, inclusive guias orientativos e recomendações expedidos pela ANPD
2. Executar Avaliação Interna de Riscos à Privacidade (AIRP)
3. Avaliar lições aprendidas
   3.1. Propor novo ciclo DPMS, para o ano seguinte
4. Realizar pesquisa interna sobre PD&P
   4.1. Realizar pesquisa com pontos focais e/ou colaboradores, para compor Relatório de Autoavaliação

ENTREGAS ETAPA 05:

- Relatório de monitoramento de leis e demais normas sobre privacidade e proteção de dados pessoais;
- Relatório de Avaliação Interna de Riscos à Privacidade (AIRP);
- Relatório de mudanças a serem propostas para o próximo ciclo de execução do DPMS;
- Relatório de Autoavaliação.

10. Benefícios e resultados esperados

A Lei Federal n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) estabeleceu mudanças fundamentais na forma como as empresas (e mesmo as pessoas físicas, em alguns casos) devem lidar com dados pessoais. Os negócios devem observar a proteção dos dados pessoais e da privacidade de seus clientes, funcionários, dentre outros, cumprindo as obrigações a eles inerentes, para que estejam em conformidade (compliance) com a legislação em vigor.

Para que a proteção de dados pessoais seja incorporada às diversas atividades executadas pelos mais diversos perfis de negócio, recomenda-se a adoção de um programa de conformidade (ou governança) em privacidade, conforme as melhores práticas adotadas no Brasil e no exterior.

A Consultoria visa a adequar a empresa à LGPD, e dentre os possíveis benefícios estão:

- Relatório de Maturidade com o respectivo mapa de calor;
- Análise do nível de aderência da empresa em relação à legislação;
- Inventário de dados pessoais;
- Identificação dos pontos de melhoria;
- Definição de processos de governança e proteção de dados pessoais conforme o nível de maturidade e segmento da empresa;
- Documentos e relatórios necessários à gestão do Programa de Conformidade;
- Atendimento às solicitações doss titulares de dados pessoais.

11. Estrutura e materiais necessários

Internet, processos da empresa mapeados, leis e regulamentos que a empresa precisa cumprir e formulários de coleta de dados.

12. Responsabilidades da empresa demandante

1. Aprovar a proposta do Sebrae, valores e condições de pagamento.
2. Conhecer e validar a proposta de trabalho, o escopo das etapas e as entregas da prestadora de serviço.
3. Disponibilizar agenda prévia para visitas, reuniões e atividades propostas pela prestadora de serviço.
4. Fornecer informações técnicas sobre os processos, produtos ou serviços à prestadora de serviço para o desenvolvimento do trabalho.
5. Acompanhar a prestadora de serviço em visita(s) técnica(s) aos espaços físicos, se previsto no escopo do trabalho.
6. Avaliar o serviço prestado.

13. Responsabilidade da prestadora de serviço

1. Realizar reunião para alinhamento e apresentação das atividades previstas.
2. Analisar a demanda e as informações fornecidas pela empresa.
3. Elaborar proposta, escopo de trabalho, cronograma das etapas do trabalho, agenda de reuniões e atividades, sendo necessário validar com a empresa demandante.

4. Fornecer as entregas previstas, validadas pela empresa demandante, ao Sebrae.
5. Cumprir com as obrigações previstas no Regulamento do Sebraetec.
6. Atuar com confidencialidade e não armazenar cópias ou dados de informações dos clientes da empresa demandante, obedecendo também todas as regras da LGPD.

14. Perfil desejado da prestadora de serviço

Empresas com experiência em segurança da informação, proteção de dados pessoais e atuação na adequação de processos à LGPD.

15. Pré-diagnóstico

1. A empresa tem como objetivo se adequar à Lei 13.709/2018 – LGPD?
2. A empresa tem conhecimento da forma que pode ser impactada pela não adequação à LGPD?
3. A empresa se insere no conceito de agente de tratamento de pequeno porte, previsto pelo art. 2º, I, da Resolução ANPD n. 2/2022?
4. A empresa se relaciona diretamente com o consumidor final?
5. A empresa possui práticas de governança relacionadas a proteção de dados?
6. Seus colaboradores conhecem os princípios básicos da LGPD, gerando segurança no fornecimento de dados pessoais por parte de seus clientes?
7. Sua empresa conhece as penalidades e multas decorrentes da não adequação de sua empresa à LGPD?
8. Sua empresa possui arquivos em meio físico com dados pessoais de clientes e/ou colaboradores?
9. Quais procedimentos de segurança da informação sua empresa realiza?

16. Observações

1. Na impossibilidade de esta ficha técnica ser aplicada presencialmente, ela poderá ser aplicada de forma remota (ferramentas de videoconferência, ligações telefônicas, aplicativos de mensagens e/ou e-mails). No momento da contratação, a empresa demandante deverá ser comunicada que parte do serviço ou a integralidade dele, quando aplicável, acontecerá de forma remota. Além disso, o alinhamento do formato do atendimento deve ser feito na Etapa 01 entre a empresa demandante e a prestadora de serviço tecnológico;
2. Na impossibilidade de as entregas serem assinadas fisicamente pela empresa demandante, elas poderão ser validadas via assinatura digital, aceite eletrônico ou e-mail, em que a empresa demandante deverá manifestar o aceite e encaminhar para a prestadora de serviço tecnológico, e esta deverá incluir o comprovante de validação da empresa demandante nas entregas para o registro do atendimento;

3. Os valores dos honorários apresentados pela prestadora de serviço devem incluir todas as despesas com impostos e encargos sociais, conforme legislação tributária em vigor, que possam incidir sobre o objeto da proposta;
4. Despesas adicionais com terceiros (direitos autorais, fotografias, hospedagem, imagens, registro de domínio, revisões, textos, conteúdo dinâmico, entre outros) ficam a cargo exclusivo da empresa demandante e devem ser previamente autorizadas por ela durante a validação da proposta de trabalho.
5. É de responsabilidade da prestadora de serviço todo o trabalho, da concepção à aprovação da empresa demandante.
6. A prestadora de serviço não pode ser responsabilizada por erros de terceiros contratados pela empresa demandante.

HISTÓRICO DE ALTERAÇÕES			
Versão	Data	Link	Responsável
1	24/09/2020	https://datasebrae.com.br/wp-content/uploads/2021/03/Adequação-à-Lei-Geral-de-Proteção-de-Dados-LGPD-GQ13070-1.pdf	Eduardo Cardoso Garrido Eder Max de Oliveira Arthur Guimaraes Carneiro
2	31/03/2021	https://datasebrae.com.br/wp-content/uploads/2021/09/Adequação-à-Lei-Geral-de-Proteção-de-Dados-LGPD-GQ13070-2.pdf	Arthur Guimaraes Carneiro Eder Max de Oliveira
3	24/09/2021	https://datasebrae.com.br/wp-content/uploads/2021/09/Adequação-à-Lei-Geral-de-Proteção-de-Dados-LGPD-GQ13070-3.pdf	Arthur Guimaraes Carneiro Eder Max de Oliveira
4	23/09/2022	https://datasebrae.com.br/wp-content/uploads/2022/09/Adequação-à-Lei-Geral-de-Proteção-de-Dados-LGPD-GQ13070-4.pdf	Coordenação Sebraetec
5	19/12/2022	https://datasebrae.com.br/wp-content/uploads/2022/12/Adequacao-a-Lei-Geral-de-Protecao-de-Dados-LGPD-GQ13070-5.pdf	Coordenação Sebraetec