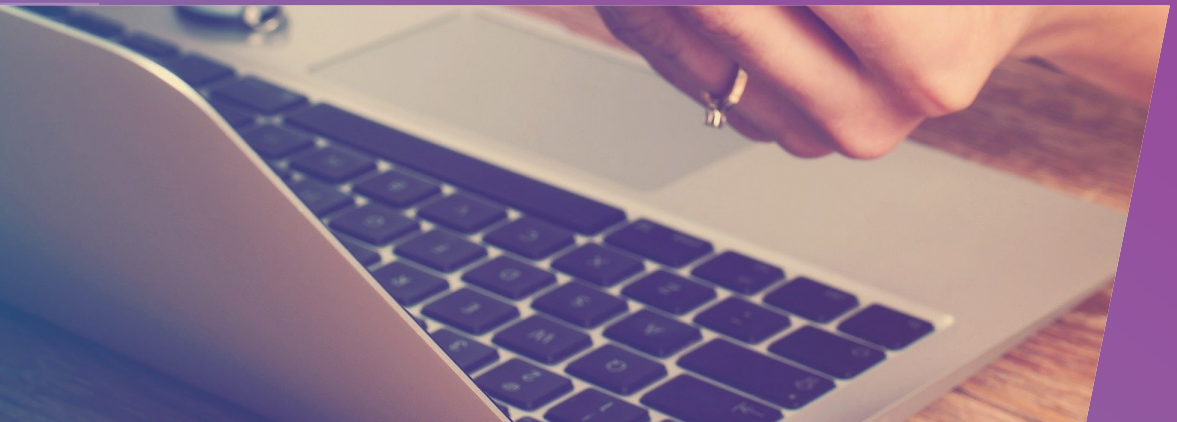
CONSULTORIA

LGPD para empresas



SEBRAE

Sumário

Apresentação

Não é de hoje que os países mais desenvolvidos estão preocupados com a proteção de dados. A Europa já está há quatro décadas discutindo o tema e a Alemanha é considerada como o berço da proteção de dados.

No Brasil o tema foi discutido pelos parlamentares durante 8 anos e só em 14 de agosto de 2018, a Lei 13.709/2018 – Lei Geral de Proteção de Dados – foi sancionada. A LGPD altera o Art. 7° da Lei 12.965 de 23 de abril de 2014, Lei de Acesso à Internet, que trata dos direitos assegurados ao usuário.

Com advento da Lei, há uma mudança considerável na utilização dos dados dos consumidores, as empresas terão que ter mais atenção quanto ao compartilhamento de informações pessoais, bem como devem criar mecanismos de controle e utilização. O consumidor passa a ser o proprietário de seus dados pessoais e as empresas precisam de autorização para divulgação e compartilhamento.

A proteção dos dados será necessária em todas as situações que haja utilização de dados pessoais, sejam nas vendas on-line, nas redes sociais, nos aplicativos de celulares, no comércio local, todos serão afetados com a Lei de Proteção de Dados Pessoais (LGPD).

Na percepção do profissional Fabricio da Mota, membro da Comissão Especial de Proteção de Dados do Conselho Federal da OAB, que contribuiu com a elaboração da PEC n° 17/2019, que propõe que a proteção de dados pessoais seja um direito fundamental do indivíduo, para a Lei Geral de Proteção de Dados, é necessário que as informações sejam percebidas por especialistas não só da área jurídica, como também pessoas com especialidade em áreas como segurança e tecnologia da informação, administração e comunicação.

Mesmo com a publicação da LGPD, o empresário não deve esquecer de observar o Código de Defesa do Consumidor, a Lei de Acesso à Informação, e o Marco Civil da Internet.

Em pesquisa realizada pela Fundação Getúlio Vargas e o SEBRAE os pequenos negócios representam 51% dos empregos gerados, principalmente nos setores de comércio e serviço e representam 30% do PIB nacional.

Com tanta representatividade no cenário econômico, o SEBRAE busca apoiar os pequenos negócios na implementação de controles gerenciais eficientes, o que não pode ser diferente quando se fala na proteção dos dados de seus clientes, buscando disponibilizar informações para que possam entender seus direitos e obrigações, como responsável por uma base de dados pessoais, seguindo um caminho de conformidade legal, mas principalmente, tendo como diferencial do seu negócio, a preocupação com seus clientes.

Ficha Técnica

FORMATO
Consutoria para Diagnóstico Empresarial

NOME
Diagnóstico da Lei Geral de Proteção de Dados - LGPD.

COMPETÊNCIAS GERAIS

COGNITIVAS
- Compreender a necessidade de cumprir com os requisitos da Lei Geral de Proteção de Dados, quanto à utilização de dados pessoais de seus clientes, evitando sanções.

ATITUDINAIS
- Predispor-se à organizar a empresa, criando procedimentos internos, de acordo com os fundamentos da LGPD.

OPERACIONAL
- Implementar uma política de segurança, criar um controle de gestão dos dados que atenda às condições legais do consumidor, treinando a equipe para minimizar ocorrências e possíveis falhas.

PÚBLICO-ALVO
Microempreendedores Individuais, Microempresas e Empresas de Pequeno Porte.

GRAU DE ESCOLARIDADE EXIGIDO
Fundamental incompleto

CARGA HORÁRIA
10 horas

MODALIDADE
P – Presencial ou D - Distância

CONTEÚDO DA CONSULTORIA

- Base legal da Lei nº 13.709/2018 – LGPD
- O papel da empresa
- O papel do controlador
- Elaboração de uma política de segurança
- Política de privacidade
- Metodologia de aplicação
- Conceitos

PERFIL DO EDUCADOR

FORMAÇÃO E EXPERIÊNCIA:

- Formação superior nas áreas de Direito.

ÁREA DE CONHECIMENTO:

- Legislação aplicada às Micro e Pequenas Empresas.

SUBÁREAS:

- Direito Empresarial.

CONHECIMENTOS NECESSÁRIOS:

- Referenciais Educacionais do Sebrae;
- Conhecimento em Diagnóstico Empresarial;
- Conhecimento sobre o Código de Defesa do Consumidor, a Lei de Acesso à Informação e o Marco Civil da Internet;
- Capacidade de interpretar a legislação para o empresário.

HABILIDADES E ATITUDES DESEJÁVEIS:

Autodesenvolvimento: posicionamento pró-ativo, de forma a construir continuamente o seu processo de aprendizagem.

Comunicação oral e escrita: expressão de ideias de maneira clara (fluência correta, riqueza de vocabulários e dicção), paraverbais (modulação, timbre, ritmo, volume e entonação da voz) e não verbais (gestos, postura e expressões corporais).

Credibilidade: coerência entre discurso e prática, inspirando no outro confiança na sua capacidade pessoal e profissional.

Empatia: capacidade de analisar situações do ponto de vista do outro, percebendo suas necessidades e valores de modo a possibilitar um entendimento mútuo.

Flexibilidade: prontidão para mudar atitudes e redirecionar comportamentos, bem como para se adaptar aos recursos disponíveis.

Motivação: expressão do interesse, entusiasmo e envolvimento com a atividade.
Organização: administração do tempo e recursos disponíveis de forma prática e racional.

Percepção: capacidade de processar e captar mensagens explícitas e implícitas das pessoas e do grupo.

Respeito: comportamento socialmente adequado, com educação e considerando o trato com as pessoas.

Visão sistêmica: visão ampliada, contextualizada e atualizada do Sebrae e do ambiente empresarial da MPE.

LISTA DE MATERIAIS

MATERIAL DO PARTICIPANTE

- CARTILHA SOBRE A LGPD
- FORMULÁRIO DE APLICAÇÃO DO DIAGNÓSTICO

OUTROS

- 01 LISTA DE REGISTRO DA VISITA

Fundamentação Teórica

A Lei Geral de Proteção de Dados – LGPD Lei nº 13.709/2018, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

(http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm)

A Lei não se aplica:

- Para fins particulares e não econômicos, realizados pelo cidadão comum;
- Fara fins jornalísticos e artísticos;
- Para fins acadêmicos, desde que sejam obedecidos os art. 7º e 11º, que dispõe dos requisitos do tratamento de dados pessoais e sensíveis;
- Pelo poder público, relacionado à segurança pública, defesa nacional, segurança do próprio Estado, investigações e crimes penais.

Em de 08 de julho de 2019, foi publicada a Lei º 13.853 com alterações - veto parcial – na LGPD:

- § 3º do art. 20 da Lei nº 13.709, de 14 de agosto de 2018, alterado pelo art. 2º do projeto de lei de conversão;
- Inciso IV do art. 23 da Lei nº 13.709, de 14 de agosto de 2018, alterado pelo art. 2º do projeto de lei de conversão;
- § 4º do art. 41 da Lei nº 13.709, de 14 de agosto de 2018, alterado pelo art. 2º do projeto de lei de conversão; Inciso V do art. 55-L da Lei nº 13.709, de 14 de agosto de 2018, inserido pelo art. 2º do projeto de lei de conversão;
- Incisos X, XI e XII, §§ 3º e 6º do art. 52 da Lei nº 13.709, de 14 de agosto de 2018, alterados pelo art. 2º do projeto de lei de conversão.

(https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=13853&ano=2019&ato=9a5ETU61keZpWT91e)

BASE LEGAL	PRINCÍPIOS
Lei 13.709/2018 LGPD	Finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.
Lei 13.853/2019	Alteração na redação e veto parcial.
Lei 12.965/2014 Marco da Internet	Garantia da liberdade de expressão, privacidade, proteção dos dados pessoais, neutralidade de rede, estabilidade e segurança da rede, responsabilização dos agentes, preservação da natureza participativa da rede e liberdade dos modelos de negócios na internet.

2.1 SÍNTESE DA LEI Nº 13.709/2018

ARTIGOS	DESCRIÇÃO
Art. 2º	Dispõe sobre os fundamentos: privacidade; autodeterminação informativa (controle dos dados pessoais); liberdade de expressão; inviolabilidade da intimidade, honra e imagem; desenvolvimento econômico;
Art. 3º e 4º	Aplica-se ao tratamento de dados da pessoa natural por pessoa física ou pessoa jurídica, desde que sejam utilizados para fins econômicos. Exclui-se da Lei, os fins: acadêmico, exclusivo de segurança pública, defesa nacional, segurança do Estado ou atividades investigativas.
Art. 5º	Define o que é: dados pessoais, sensíveis, anonimizado/ anonimização, banco de dados, titular, controlador, operador, encarregado, tratamento, consentimento, bloqueio, eliminação, transferência internacional e dados, uso compartilhado de dados, relatório de impacto e órgão de pesquisa.
Art. 6º	Dispões sobre os princípios: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas
Art. 7º, 8º, 9º e 10º	Dispõe sobre os requisitos para o tratamento, além das hipóteses para esta realização: consentimento, obrigação legal; administração pública, quando se tratar de políticas púbicas; estudos e pesquisas; contratos do titular ou que seja parte dele; proteção da vida; tutela da saúde; proteção do crédito. Quando o titular manifesta que seus dados podem ser públicos, mesmo que uma dispensa eventual do consentimento, ainda assim não desobriga os agentes de tratamento das demais obrigações previstas na Lei. Cabe ao controlador a responsabilidade de provar que há consentimento no tratamento e divulgação dos dados. O consentimento pode ser revogado a qualquer momento pelo titular e seu acesso às informações deve ser facilitado.

Art. 11º, 12º e 13º	Estabelece sobre o tratamento de dados pessoais sensíveis com suas hipóteses, formas de aplicação e garantias de utilização de forma adequada. Define que os dados anonimizados não serão considerados dados pessoais, descrito na Lei em artigo específico.
Art. 14º	Estabelece sobre o tratamento de dados pessoais de crianças e adolescentes.
Art. 15º e 16º	Estabelece o prazo para utilização dos dados por meio dos agentes de tratamento.
Art. 17º, 18º, 19º, 20º ,21º e 22º	Dispõe sobre os direitos do titular, de acordo com os fundamentos da liberdade, intimidade e privacidade, a forma consentimento e revogação do direito de utilização por parte dos agentes de tratamento. Proíbe a utilização dos dados em prejuízo do titular.
Capítulo IV	Cria regras de tratamento de dados pessoais pelo Administração Pública
Capítulo V	Estabelece que a transferência internacional de dados seja feita somente para países ou organismos internacionais que possuam grau de proteção adequado por Lei.
Art. 37º, 38º, 39º, 40º e 41º	Define sobre o papel do controlador, do operador e do encarregado pelo tratamento de dados pessoais.
Art. 42º, 43º, 44º e 45º	Dispõe sobre a responsabilidade e ressarcimento de dados, caso ocorra danos ou violação à legislação.

At. 46º, 47º, 48º e 49º	Dispõe sobre as medidas de segurança e sigilo dos dados pessoais pelos agentes de tratamento, seguindo padrões técnicos mínimos, além das providências pela Autoridade Nacional de Proteção de Dados para verificação dos incidentes e salvaguarda do direito dos titulares.
Art. 50º e 51º	Dispõe sobre as regras de boas práticas e governança no tratamento de dados pessoais. Estabelece que as empresas deverão verificar a probabilidade e a gravidade dos riscos decorrentes do tratamento dos dados pessoais. As empresas devem ter um programa de governança em proteção de dados que seja efetivo e que não cause danos aos titulares dos dados. As regras de boas práticas e governança deverão ser publicadas e atualizadas periodicamente.
Art. 52º, 53º e 54º	Estabelece que as empresas que não cumprirem com os requisitos da LGDP, estarão sujeitas às sanções, de acordo com o nível de prejuízo causado ao titular dos dados pessoais. As sanções administrativas vão da advertência, com adoção de medidas corretivas a uma multa simples de 2% sobre o faturamento da empresa, limitada à R$ 50 milhões por infração.
Art. 55-A (texto modificado pela Lei 13.853/2019	Cria a Autoridade Nacional de Proteção de Dados (ANPD), ainda sem regulamentação, veta parcialmente e altera o texto da Lei 13.709/2018 em alguns pontos.

O papel da empresa

A base principal da Lei Geral de Proteção de dados - LGPD é o consentimento do titular para que as empresas possam utilizar seus dados. Dá garantia de que os dados serão protegidos e somente serão utilizados para os fins a que forem destinados, garantido o direito de exclusão, quando o titular não mais quiser disponibilizá-lo.

Com o advento da Lei, há um impacto direto nos pequenos negócios, que deve se adequar para esta nova realidade.

Todos os dados pessoais de seus clientes deverão ser tratados e de acordo com o Art. 6º da LGPD, seguindo os princípios de:

- Finalidade: o tratamento e utilização dos dados devem ser utilizados com fins específicos, não podendo haver mudança na utilização desses dados, sem o consentimento do indivíduo. Devem ser observados, os princípios da Lei

- Adequação: Os dados só poderão ser utilizados de acordo com a finalidade e devem ser compatíveis com a autorização dada pelo proprietário daqueles dados. Não poderá haver mudança na destinação dos dados, sem que haja consentimento.

- Necessidade: a utilização dos dados deve estar estritamente relacionada ao fim em que foi definido.

- Livre acesso: o proprietário deve ter livre acesso para consultar seus dados, como serão utilizados e garantia de que as informações não serão distorcidas ou modificadas.

- Qualidade: a utilização dos dados deve ser da forma mais fidedigna, é necessário cuidado com sua utilização, com clareza e sempre com finalidade que foi definido.

- Transparência: garantia de que os dados serão divulgados de forma clara, precisa e transparente. Não podem ser enviados a terceiros.

- Segurança: são as medidas de proteção que deverão ser utilizadas para garantir que os dados não sejam adulterados, modificados ou perdidos.

- Prevenção: são todas as medidas adotadas para que sejam evitados danos e virtude do tratamento dos dados.

- Não discriminação: jamais pode haver utilização dos dados de forma discriminada ou ilícita.

- Responsabilização e prestação de contas: os responsáveis pela utilização de dados pessoais são obrigados a prestar contas, quando necessário, e serão responsabilizados, caso haja má utilização dos dados. É necessário adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais.

As empresas deverão criar um controle de gestão dos dados que atenda às condições legais do consumidor, não poderá haver compartilhamento de dados pessoais sem a autorização do titular e a qualquer momento, a pedido do cliente, poderá solicitar o cancelamento deste compartilhamento. Assim, a necessidade de organizar os dados de seus clientes e o responsável por estes dados tem que estar bem definido.

O tamanho da base de dados fará com que a empresa tenha maior ou menor controle de gestão.

De acordo com o art. 18° da LGPD, a empresa que possui uma equipe de funcionários, deverá definir quem será o operador, responsável por fazer o tratamento e a gestão dos dados, a partir de um controle, mantendo um registro das operações atualizado, que servirá de base para o Relatório de impacto à proteção de dados, de responsabilidade do controlador com informações sobre sua destinação, tratamento, riscos e formas de proteção. O controlador poderá definir um encarregado para ser o canal de comunicação com a Autoridade Nacional de Proteção de Dados, que poderá solicitar que seja apresentado um relatório.

Obs: A ANPD ainda está em fase de estruturação, assim os Estados, Municípios e Distrito Federal ainda não possuem um órgão fiscalizador local. O modus operantis da fiscalização ainda não foi definido.

Estados e Municípios devem estar atentos às legislações locais.

3.1. OS PRINCIPAIS IMPACTOS DA LEI PARA AS MPEs

3.1.1. O impacto da captação e manutenção dos dados dos clientes:

O que fazer?

1) A empresa precisa identificar as Bases Legais para sua Carteira de Clientes. Isto é, precisa ter sua base dados enquadrada em, pelo menos, uma das 10 hipóteses previstas na LGPD, para registrar dados e se relacionar com sua clientela, quais sejam:

- O consentimento do titular;
- O legítimo interesse;
- A execução de Políticas Públicas;
- A realização de estudos por órgãos de pesquisa;
- A execução de contrato de qual seja parte o titular;
- O exercício regular do direito em processo judicial, administrativo ou arbitral;
- A proteção à vida;
- A tutela da saúde;
- O cumprimento de obrigação legal ou regulatória pelo controlador;
- A proteção ao Crédito.

2) A empresa precisa definir uma estratégia de ação, de acordo com o seu negócio, de modo a conseguir os dados de seus clientes que precisam ser registrados e tratados. Isso exigirá a construção de uma política de captação, proteção e segurança de dados concisa e escrita em linguagem acessível, para que as pessoas ou clientes possam compreender e confiar no que sua empresa está comunicando.

Para atingir esse objetivo, que sua empresa precisará?

1) Fazer o mapeamento e validação dos dados registrados na empresa, definindo os que são realmente essenciais para o seu negócio, envolvendo:

- Informações sobre o responsável pelo tratamento;
- Dados pessoais e respectivas finalidades do tratamento, inclusive os dados não informados pelo usuário (exemplo: IP, localização, cookies, etc.);
- Elencar a base legal (Base Jurídica do Tratamento) identificando as hipóteses de enquadramento para uso dos dados essenciais para finalidade da empresa.
- Estabelecer o prazo de retenção dos dados pessoais;

- Definir o Data Protection Officer (DPO), encarregado de proteção de dados da organização e manter às informações de contato disponíveis aos clientes e colaboradores.

2) Elaborar processo de obtenção do consentimento para uso dos dados de cada cliente, definindo o uso específico e assegurando a segurança deles.

- **Princípio da Finalidade**
  O consentimento deve ser fornecido para uma determinada finalidade. Isto é, o consentimento deve ser específico. Se você possui mais de uma empresa com finalidades distintas, você não poderá usar a mesma base da dados para ambas as empresas. Ex. enviar mensagens para clientes de empresas distintas usando a mesma base de dados. Cada empresa deverá obter o consentimento para sua finalidade.

- **O cliente deve ter a possibilidade de escolha livre para dar ou não o consentimento.**
  A empresa não pode condicionar ou aglutinar em um mesmo consentimento Termos de Uso, Políticas de Privacidade e envio de mensagem promocionais, por exemplo.

- **A compra de e-mails de potenciais clientes (estratégia de outbound marketing) podem ser ilegais de acordo com a LGPD.**
  Isto infringe o princípio do consentimento por parte das pessoas para que uma empresa comercialize seus dados com outras empresas. E infringe o princípio da finalidade, pelo fato de a pessoa não saber que uso o comprador de listas fará com seus dados, podendo tanto a empresa vendedora quanto a empresa compradora serem responsabilizadas legalmente.

- **Usar solicitação de consentimento online para os aceites imediatos na medida das necessidades.**
  Enviar ou e-mail ou mensagem solicitando a autorização para uso específico. Ter também, a opção de colher o consentimento na forma presencial, com base em formulário impresso.

- **Se você usa sistema informatizado, não se esqueça dos cookies.**
  Os cookies utilizados no navegador, que podem ser considerados dados pessoais. Por exemplo, se o uso dos cookies autorizados para um acesso for usado para outra finalidade (tipo campanhas promocionais), esse ato enquadrará os registros dos cookies com dados pessoais, visto que o cliente pode ser impactado por uma campanha, para qual ele não autorizou o uso

de seus dados. Assim, caso necessário, será preciso obter autorização para essa nova finalidade.

- **Facilitar a saída ou descredenciamento das pessoas ou clientes registrados em suas bases de dados.**
  Dificultar a saída da pessoa, pode ser enquadrado como um ato de descumprimento da LGPD. O cliente, contato ou lide deve poder sair de sua base de dados com a mesma facilidade com que entrou. Assim, os procedimentos de descredenciamento, ou saída do cadastro de cliente deve ser o mais transparente possível.

- **Manter o cadastro de clientes ou lides organizado, por segmento de preferência, de forma a facilitar o estabelecimento de boas práticas de automação.**
  Embora a LGPD não inviabilize a tomada de decisão automatizada, deve-se evitar a ocorrência de práticas discriminatórias ou invasivas. Por exemplo, utilizar o resultado de uma análise de crédito para ofertar empréstimos facilitados, mas com juros mais altos que os praticados no mercado, para pessoas com dificuldades financeiras, é um tipo de prática não aceita pelo regramento da LGPD.

3.1.2. O impacto na Análise e Proteção desses Dados Pessoais:

O que fazer?

1) Sua empresa poderá precisar investir também na garantia à proteção efetiva dos dados registrados em suas bases de dados e tornando-as seguras, de modo que não haja possibilidade de violação. Isto porque a violação gera sanção e pode gerar prejuízo financeiro. Algumas ações importantes para isso são:

- De acordo com o nível de informatização atual, a empresa poderá investir na aquisição de soluções de segurança automatizadas, com funcionalidades adequadas a seu perfil de consumo de dados.

- Estabelecer o uso de Boas Práticas de Segurança Cibernética:

- Proibir o uso de pen drives;

- Difundir o uso de senhas complexas, que sejam periodicamente trocadas;

- Estabelecer níveis de acesso;
- Manter um filtro de spam atualizado;
- Não acessar a rede Wi-Fi da empresa para atividades particulares no celular;
- Dar preferência ao uso de nuvem segura como forma de compartilhar os documentos.

3.1.3. Os impactos na Rotina dos Colaboradores da Empresa:

O que fazer?

1) Manter um programa de capacitação dos colaboradores sobre a legislação, segurança e boas práticas, é essencial;

2) Com a LGPD, passa a ser responsabilidade de todo o corpo de colaboradores conhecer as bases legais e se manter atualizado e atento, para a prevenção de eventos que possam afetar a empresa. Tudo isso para garantir que os clientes se sintam seguros em fornecer os dados e a empresa tenha a base de dados com abrangência ideal para o negócio;

3) Estabelecer um Política de Segurança e Boas Práticas é fundamental, para o alcance desse objetivo.

3.1.4. O impacto nas Finanças da Empresa:

Nesse caso as opções são:

1) A empresa ter um custo com as adequações e manutenção da conformidade com a LGPD;

2) A empresa ter um custo com multas e penalidades. Isto posto, entendemos que é melhor investir em prevenção, na proteção dos dados dos clientes e ter uma base de dados segura, do que arriscar para penalidades que podem alcançar 2% do faturamento chegando à R$ 50 mil, valendo sempre o maior valor apurado entre essas duas opções.

O papel do controlador

De acordo com o art. 5º, o controlador é a pessoa natural ou jurídica, denominado agente de tratamento, com a competência de tratar os dados pessoais. Cabe ao controlador o ônus da prova de que o consentimento de utilização dos dados foi obtido junto ao cliente, em conformidade com o disposto na lei.

É necessário que Controlador cumpra com os requisitos do art. 9º, para atendimento do princípio do livre acesso, onde o titular dos dados tem o direito de obter informações sobre a identificação do controlador, suas responsabilidades e formas utilizadas para o tratamento dos dados.

De acordo com o art. 18º da Lei, a empresa tem o direito de obter, a qualquer momento, que dados forem utilizados, seu tratamento, se houve compartilhamento, eliminação, a anonimização ou o bloqueio dos dados, exigindo dos potenciais parceiros que repitam idêntico procedimento.

O Controlador é o responsável:

- Manter o registro das operações de tratamento de dados em conjunto com o operador, baseado no legítimo interesse;
- Indicar o encarregado;
- Em exercício da atividade, caso cause dano patrimonial, moral, individual ou coletivo, é obrigado a repará-lo, se não forem observadas as medidas de segurança previstas no art. 46º; Caso o operador esteja diretamente envolvido no tratamento em houver dano ao titular dos dados, responde solidariamente;
- Comunicar à autoridade nacional e ao titular a ocorrência de incidência de segurança;
- Definição de mecanismos de proteção de dados;
- Formular regras de boas práticas e de governança dos dados.

A Lei também traz o papel do operador, que realiza o tratamento de dados pessoais em nome do controlador. E o encarregado, pessoa indicada pelo controlador, para atuar como canal de comunicação entre o controlador e a Autoridade Nacional de Proteção de Dados.

Elaboração de uma política de segurança

O objetivo de uma Política de Segurança da Informação - PSI visa estabelecer princípios e diretrizes para assegurar a confidencialidade, integridade e disponibilidade dos dados e dos sistemas de informação utilizados, garantindo a proteção adequada dos ativos e dos dados.

Tais medidas garantem, também, a identificação, proteção, detecção, resposta e recuperação de eventos em casos de eventual incidente de segurança.

5.1. Princípios da Segurança da Informação

O compromisso com o tratamento adequado das informações de clientes e público em geral está fundamentado nos seguintes princípios:

I. Confidencialidade: garantir que a informação não estará disponível ou divulgada a indivíduos, entidades ou aplicativos sem autorização. Em outras palavras, é a garantia do resguardo das informações dadas pessoalmente em confiança e proteção contra a sua revelação não autorizada.

II. Integridade: garantir que a informação não seja alterada em seu conteúdo e, portanto, é íntegra, autêntica, procedente e fidedigna.

III. Disponibilidade: permite que a informação seja utilizada sempre que necessário, estando ao alcance de seus usuários.

5.2. Ciclo de Vida da Informação

Para efeito de política, deve ser considerado o seguinte ciclo de vida da informação:

I. Manuseio: é a etapa onde a informação é criada e manipulada.

II. Armazenamento: consiste na guarda da informação, seja em um banco de dados, em papel, em mídia eletrônica interna ou externa, entre outros.

III. Transporte: ocorre quando a informação é transportada de um local para outro, não importando o meio no qual ela está armazenada.

IV. Descarte: refere-se à eliminação de documento impresso, eliminação de arquivo eletrônico ou destruição de mídias de armazenamento (por exemplo, CDs, DVDs, disquetes, pen-drives).

5.3. Níveis de Acesso aos Dados

O processo de controle de acesso à informação visa garantir que o acesso físico e lógico à informação seja franqueado exclusivamente a pessoas autorizadas, com base nos requisitos de negócio e de segurança da informação.

A organização deve estabelecer em seus contratos, acordos, convênios ou ajustes, cláusulas específicas sobre sigilo, em especial quando informações forem disponibilizadas à terceiros, que assegurem a observância da LGPD.

A definição dos níveis de acesso deve considerar três aspectos:

- **Quem acessa?**
  Devem ser definidos os cargos ou as pessoas de determinadas funções que podem acessar os dados. Isso garante que um gestor de RH ou um vendedor sempre tenha acesso ao mesmo número de informações necessário para a execução de suas tarefas diárias.

- **Como acessa?**
  Por meio de quais sistemas e dispositivos o titular poderá acessar os dados.

- **Quando acessa?**
  Fora do horário de expediente ou de sua jornada de trabalho, a pessoa pode consultar os dados?

5.4. Controles Internos de Segurança da Informação

5.4.1. Identificação/Avaliação de Ameaças e Vulnerabilidades

É a identificação e avaliação dos riscos a que os processos e ativos relevantes estejam sujeitos em virtude das vulnerabilidades e possíveis cenários de ameaça atribuídos a cada processo ou ativo.

Os equipamentos, os sistemas e os aplicativos da organização precisam ser regularmente avaliados e atualizados.

É necessário investir em práticas de segurança para cada componente da infraestrutura.

5.4.2. Ações de Prevenção e Proteção

Sem prejuízo de ações específicas para proteção e prevenção de riscos identificados e avaliados, devem ser adotadas rotinas padronizadas de prevenção e proteção dos processos e ativos, realizando análises de vulnerabilidade, testes de intrusão e outras avaliações específicas que certifiquem o cumprimento dos requisitos de segurança e as responsabilidades previamente estabelecidas.

5.4.3. Monitoramento e Testes

Devem ser implementados controles internos efetivos para proteção dos Recursos de Tecnologia da Informação e Comunicação, garantindo a sua confidencialidade, integridade, disponibilidade, com as melhores práticas de mercado e regulamentações vigentes.

Os aplicativos críticos devem implementar a geração/manutenção de trilhas de auditoria, controle de versionamento do código fonte e segregação entre os ambientes de produção, homologação e teste. As ameaças cibernéticas devem ser analisadas e devem possuir monitoramento proativo.

5.4.4. Plano de Ação e de Resposta a Incidentes

Os incidentes de segurança da informação devem ser identificados e registrados para acompanhamento pelos planos de ação e análise das vulnerabilidades.

Os incidentes deverão ser avaliados e investigados de forma a construir uma análise consistente de causas-consequências, riscos envolvidos, partes envolvidas e planos de respostas. Deverá ser emitido, tempestivamente, comunicado às partes envolvidas informando a situação ocorrida e ações definidas, ainda que preliminares, informando/notificando as atividades posteriores pertinentes.

Um Plano de Ação deverá ser elaborado para implementação das soluções para administração de eventuais contingências e continuidade pós incidente. Tal plano deve contar com definição expressa dos papéis e responsabilidades na solução do impasse. O Plano de Ação deverá, ainda, prever os casos de necessidade de utilização das instalações de contingências nos casos mais severos.

Os Sistemas de Informação, além de disponibilizar os registros em prazos e formatos que atendam às exigências legais, devem protegê-los contra perda, acesso indevido, destruição e falsificação, visando à salvaguarda dos dados

5.5. Sistema de Gestão da Segurança da Informação

Deve-se estabelecer um Sistema de Gestão da Segurança da Informação (SGSI) que é um conjunto de disciplinas, deveres e boas práticas para estabelecer, implementar, operar, monitorar, revisar, manter e aprimorar a segurança da informação visando a coordenação de ações em quatro grandes frentes de atuação:

I. Governança das políticas e procedimentos de segurança da informação;
II. Recursos e componentes de segurança da informação;

III. Monitoramento contínuo do ambiente de tecnologia da informação;

IV. Gestão de crises e continuidade de negócios.

5.6. Elaborando a Política de Segurança

Para definir e implementar uma PSI é importante definir as pessoas ou equipes que vão ser responsáveis pela elaboração, implantação e manutenção da política. Da mesma sorte, definir as responsabilidades de cada equipe/pessoa, e trabalhar em conjunto com pessoas da alta administração da organização para aprovação da política e de fato obter maior respeito dos colaboradores que passarão também a conhecer a política.

Devem ser planejados procedimentos apropriados para garantir a conformidade e o respeito às exigências legais quanto à disponibilização de informações, bem como ao uso e disseminação de informações protegidas por leis tais como: dados pessoais, informações relativas à honra e à imagem, de propriedade intelectual, direitos autorais, segredos comerciais, patentes e marcas registradas ou aquelas classificadas como sigilosas.

Invista em tecnologia: os aplicativos de negócios e sistemas de TIC precisam ser adequados e configurados para garantir a aplicação da Política de Segurança da Informação - PSI, caso contrário, ela cairá em descrédito;

Divulgar e comunicar as definições e conceitos é estratégico para o sucesso da implantação da PSI;

Defina uma agenda de campanha de conscientização dos colaboradores, para relembrá-los o que não deve ocorrer dentro do ambiente interno, de forma a minimizar erros e falhas neste aspecto.

5.7. Principais fases para a elaboração de uma política

Identificação dos recursos críticos: mapear os processos da empresa e definir prioridades, importância de cada processo, estabelecendo prioridades de segurança nos processos que mais influenciam na organização;

Classificação das informações: deve-se classificar a importância da informação dentro da organização e assim definir o grau de proteção e as medidas para a sua manipulação, podendo ser confidencial, uso interno e pública;

Elaboração de normas e procedimentos: contemplando os principais aspectos de uso da infraestrutura e dos sistemas de sua organização com foco na segurança

Política de privacidade

A política de privacidade objetiva dar visibilidade ao tratamento de dados pessoais em um determinado serviço, atendendo princípios da Lei Geral de Proteção de Dados Pessoais - LGPD.

É importante garantir que a política esteja facilmente disponível. Dessa forma, a empresa demonstra profissionalmente seu compromisso com a transparência no tratamento dos dados pessoais. E o usuário deve demonstrar seu expresso consentimento e concordância com os termos da política antes do início desse tratamento.

Para a elaboração da política de privacidade, é fundamental entender o contexto do tratamento de dados pessoais e como os princípios da LGPD são atendidos no sistema ou serviço. Para tanto, é necessário mapear todos os dados pessoais, a finalidade, as bases legais que legitimam o tratamento e a forma de atendimento aos direitos do titular como acesso, retificação, exclusão, revogação de consentimento, oposição, informação sobre possíveis compartilhamentos com terceiros e portabilidade.

É fundamental também a definição dos dados, caracterizando-os como públicos, internos, confidenciais e secretos.

Para apoiar o levantamento e a análise das informações, recomenda-se usar o Questionário LGPD (Anexo) para colher e registrar as informações acima. Quaisquer alterações nessas informações devem ser refletidas em versões futuras da política.

Com relação ao conteúdo, é importante observar a presença das seguintes informações, que devem ser levantadas e registradas de modo claro e preciso:

- Informações sobre a empresa responsável pelo tratamento;
- Dados pessoais e respectivas finalidades do tratamento, inclusive os dados não informados pelo usuário (exemplo: IP, localização, etc);
- Base jurídica do tratamento;
- Prazo de retenção dos dados pessoais;
- Informações de contato do encarregado de proteção de dados da organização (Data Protection Officer (DPO).

A política de privacidade também deve orientar como são atendidos os direitos do titular de dados pessoais, apresentando como ele pode acessar, retificar, solicitar a exclusão de dados, transferir, limitar ou se opor ao tratamento, e retirar o consentimento.

Quando aplicáveis, também devem estar presentes as seguintes informações sobre:

- o compartilhamento dos dados com terceiros e qual a finalidade, inclusive redes sociais;
- a transferência internacional de dados e qual a finalidade;
- o tratamento por legítimo interesse;
- o envio de e-mail marketing e como remover o consentimento, quando autorizado inicialmente pelo titular;
- as decisões automatizadas realizadas;
- a proteção de dados de menores de idade;
- a proteção dos dados sensíveis.

6.1. Crie Uma Política Preventiva

Instrua os profissionais a agirem de maneira preventiva, a fim de evitar riscos e ataques cibernéticos e a destruição dos documentos. Entre as boas práticas, estão:

- Não permitir o uso de pen drives;
- dar preferência ao uso da nuvem como forma de compartilhar os documentos;
- manter um filtro de spam atualizado;
- Difundir o uso de senhas complexas, que sejam periodicamente trocadas;
- não acessar a rede Wi-Fi da empresa para atividades particulares no celular.
- Estabeleça níveis de acesso.

Outro fator imprescindível na política de segurança é a criação de níveis de acesso. Isso que garantirá o controle das informações. Algumas informações são restritas e precisam ser preservadas com muito cuidado.

Metodologia de aplicação

A empresa precisa se adequar para atender os requisitos da LGPD, considerando o art. 6º. Para essa adequação é necessário identificar o nível de conformidade atual da empresa em relação à Lei, para que se possa indicar recomendações para o atendimento das exigências legais, com base nas melhores práticas de mercado.

O Diagnóstico LGPD tem como objetivo permitir ao empresário ou gestor, o acesso a um processo estruturado de autoavaliação dos processos de tratamento de dados pessoais em relação aos requisitos exigidos pela LGPD, onde as respostas aos itens de avaliação serão integradas em um Relatório, que informa o nível de adequação da organização e as sugestões para os ajustes das não-conformidades.

Com base nesse Diagnóstico o empresário, poderá orientar sua equipe e realizar as adequações à Lei, com recursos humanos da própria empresa ou contratar um serviço especializado que implemente um processo de governança dos dados pessoais e seja garantidor da devida proteção e do respeito aos direitos dos titulares, nos processos de negócio da organização.

a. Partes da consultoria

Aplicação do Diagnóstico ou Autoavaliação. A proposta de Formulário usado em papel, em planilha ou em uma aplicação web, e pode ser aplicado a organizações pequenas, médias e grandes.

Está estruturado em Blocos para os quais devem ser preparadas as recomendações, de acordo com a reposta assinalada pelo empresário:

IDENTIFICAÇÃO DA EMPRESA	Informações iniciais
BLOCO I	Tratamento de dados pessoais
BLOCO II	Deveres do Controlador e do Operador
BLOCO III	Boas práticas
BLOCO IV	Recursos Humanos
BLOCO V	Tratamento de incidentes de dados pessoais
BLOCO VI	Governança de dados

Após aplicação do Diagnóstico ou autoavaliação, o consultor deverá analisar as informações e de acordo com as respostas dos empresários, é feita uma pontuação com base em um escore de 0% a 100% de conformidade, enquadrando a empresa em um dos 3 níveis abaixo:

Nível 3	Em Conformidade	de 81 a 100%
Nível 2	Em Conformidade Parcial	de 46 a 80%
Nível 1	Não Conformidade	de 0 a 45%

Considerando a tabulação das respostas e análise por parte do consultor, é necessário utilizar o modelo de relatório de devolutiva, com as orientações para a adequação da empresa aos requisitos da Lei.

Conceitos / Glossário

- **Pessoa natural:** ser humano capaz, com direitos e obrigações, desde o seu nascimento (Art. 2º do Código Civil).

- **Dados pessoais:** toda e qualquer informação relativa a uma pessoa viva, conjunto de informações distintas que podem levar à identificação de uma determinada pessoa natural (Art. 5º da LGPD).

- **Dados sensíveis:** toda informação relacionada à raça ou étnica, religião, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (Art. 5º da LGPD).

- **Dados pessoais de crianças e adolescentes:** informações relacionadas a crianças (pessoas com até doze anos incompletos) e adolescentes (aqueles que possuem de doze a dezoito anos), de acordo com o Estatuto da Criança e Adolescente – Lei nº 8.069/90. Obrigatoriamente, deve haver o consentimento dado por pelo menos um dos pais ou pelo responsável legal (Art. 14º da LGPD). O Art. 3º do Estatuto da Criança e Adolescente, trata que a criança e o adolescente dispõem de todos os direitos fundamentais inerentes a toda pessoa, também lhes sendo asseguradas todas as oportunidades e facilidades, a fim de lhes facultar o desenvolvimento físico, mental, moral, espiritual e social, em condições de liberdade e de dignidade.

- **Tratamento:** um conjunto de meios que são utilizados para classificar, processar, avaliar, controlar, divulgar e extrair informações. Para os dados pessoais, o tratamento deve levar em conta, o consentimento e a legalidade.

- **Controlador:** pessoa natural ou jurídica, de direito público ou privado, é o responsável pela tomada de decisões referentes ao tratamento de dados, caso ocorra um dano ou falha na proteção dos dados, será responsável por apresentar relatório a Autoridade Nacional, sofrendo as sanções facultadas no Art. 52º da LGPD. Poderá designar um encarregado/operador para o tratamento dos dados, que deverá ter seus dados divulgados publicamente, de forma clara e objetiva, preferencialmente no site da empresa.

- **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

- **Encarregado:** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

- **Autoridade Nacional:** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei em todo o território nacional.

- **Sanções:** São as penalidades aplicadas aos responsáveis pelo tratamento de dados, caso estejam em desacordo com a LGPD, aplicadas pela Autoridade Nacional (Art. 52° da LGPD):

  I - Advertência, com indicação de prazo para adoção de medidas corretivas;

  II - Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

  III - Multa diária, observado o limite total a que se refere o inciso II;

  IV -Publicização da infração após devidamente apurada e confirmada a sua ocorrência;

  V -Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

  VI - Eliminação dos dados pessoais a que se refere a infração.

- **Titular:** é a pessoa natural dona dos dados que serão disponibilizados, a única que pode dar o consentimento da utilização dos dados pessoais pelas empresas, garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade (Art. 17° da LGPD).

- **Consentimento:** é a manifestação favorável para a permissão de dados pessoais.

- **Eliminação de dados:** direito do titular de ter seus dados pessoais excluídos, mediante requisição, a qualquer momento (Art. 18° da LGPD). Caso haja o compartilhamento desses dados à terceiros, espera-se que o terceiro envolvido, que recebeu os dados compartilhados, também os elimine.

- **Anonimização:** manter anônimo um dado pessoal ou sensível que foi tratado para que suas informações não possam ser vinculadas ao seu titular original. "A utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado pessoal perde a possibilidade de associação, direta ou indireta, com o seu titular" (Art. 5º da LGPD).

- **Transferência internacional:** transferência de dados pessoais para outros países, desde que seja considerado que o país possui legislação que proteja os dados enviados, que comprove a garantia de cumprimento dos princípios da Lei (Art. 5º e 33º da LGPD).

- **Registro das operações:** o controlador da empresa deverá registrar as operações realizadas para o tratamento dos dados pessoais, sempre se atentando à finalidade específica da empresa (Art. 37º da LGPD).

- **Relatório de impacto à proteção de dados:** documentação do controlador que contém a descrição dos 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 (Art. 5º da LGPD).

- **Governança em privacidade:** processos e políticas internas da empresa que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais, conforme especifica a Lei (Art. 50º da LGPD).

Referências Bibliográficas

https://www.serpro.gov.br/lgpd/noticias/protecao-dados-evolucao-privacidade

https://www.alleasy.com.br/2019/10/07/lgpd-para-pequenas-empresas-como-elas-serao-impactadas/

https://datasebrae.com.br/emprego/#uf

https://www25.senado.leg.br/web/atividade/materias/-/materia/135594

http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

Anexos

TERMO DE UTILIZAÇÃO – DIAGNÓSTICO

Termos e Condições

Importante: Um Diagnóstico que tem como finalidade medir o nível de conformidade das empresas com a LGPD, precisa utilizar essa Lei como Base para sua construção. Daí a necessidade do Diagnóstico LGPD Fácil ser precedido da autorização do empresário com base em um de acordo em um Termo e Condições.

Introdução

O presente Termo e Condições destinam-se a descrever as práticas que a Ferramenta Diagnóstico LGPD segue em respeito à privacidade das informações que são concedidas, processadas e armazenadas pela mesma.

Utilização e Tipo de Informação Processada pelo LGPD

Ao acessar a LGPD serão exigidos somente os dados de sua empresa, não sendo solicitado qualquer dado ou informação que possa identificar a empresa ou qualquer tipo de dado pessoal (i.e., informação relacionada a pessoa natural identificada ou identificável) do usuário.

O fornecimento das informações para o Diagnóstico acontece de forma anonimizada e não identificável, de modo que não será necessário o fornecimento de qualquer informação da empresa e/ou pessoal que possa identificá-la, para uso da LGPD.

Para o uso do Diagnóstico é necessário responder a um questionário inicial, no qual serão solicitadas as informações sobre o porte e público-alvo, o quadro de pessoal, a região de atuação e o setor de negócios: (1) Porte da Empresa, (2) Principal Tipo de Cliente, (3) Número de Funcionários da Empresa, (4) UF onde atua e (5) Setor de Negócios.

De modo a garantir a anonimização do usuário, LGPD não armazena qualquer tipo de dado de acesso, de forma que caso o usuário saia do questionário antes de finalizá-lo, o progresso será encerrado e será necessário iniciar novamente o questionário em um novo acesso.

As informações fornecidas pelo usuário na Ferramenta poderão ser usadas por nós para fins de pesquisa e estatística, benchmarking e análise de tendências do setor, sem que haja qualquer tipo de identificação do usuário. Portanto, esteja atento para não registrar dados pessoais confidenciais ou informações confidenciais no LGPD em eventuais campos de texto livre.

O Gerenciamento do LGPD

O Ente que está agindo como Controlador de Dados, fornecendo esta ferramenta de diagnóstico, onde as informações de sua empresa serão processadas e armazenadas, o Sebrae é a uma entidade jurídica independente de apoio a micro e pequena empresa em nível nacional, com sede em Brasília, Distrito Federal, que pode atuar como um Controlador de dados em seu próprio direito. As informações que são fornecidas ao LGPD podem ser compartilhadas pelo SEBRAE com empresas e entidades de seu relacionamento, em várias jurisdições diferentes.

Quem pode acessar as informações?

O Sebrae somente irá compartilhar as informações fornecidas pelo usuário no LGPD com terceiros que concordarem expressamente, por escrito, em fornecer um nível adequado de proteção de privacidade.

As informações do usuário poderão ser acessadas no LGPD pelas seguintes categorias de pessoas para os fins abaixo descritos:

- **Administradores da LGPD :** implementar e manter a aplicação com configurações padrão, definir modelos e metadados, configurar o banco de perguntas e a lógica para ramificação que é utilizável por todos.

- **Autores de Estudos e Pesquisas:** criar questionários, gerenciar e controlar o acesso a questionários e resultados correspondentes e criar relatórios com base em resultados.

Retenção de dados

O Sebrae manterá armazenadas as informações de resposta da pesquisa no LGPD por 6 meses (ou como aprimorada/modificada pelos requisitos de política regional e local).

Dados pessoais sensíveis

O LGPD não tem o objetivo de processar dados pessoais sensíveis. Então, para atingir esse propósito, solicitamos que você não insira dados pessoais confidenciais no mesmo antes ou durante a pesquisa. Dados pessoais sensíveis significam dados pessoais de um indivíduo como os relativos a origem racial ou étnica do titular dos dados, suas opiniões políticas, suas crenças religiosas ou filosóficas, se é um membro de uma associação sindicato e sua posição, seus dados genéticos, dados biométricos, a fim de identificar exclusivamente uma pessoa, sua saúde física ou mental ou condição, a sua vida sexual e orientação, suas convicções criminais e infrações ou medidas de segurança relacionadas, seus arquivos de segurança social.

Segurança

O Sebrae usou padrões aceitos de medidas técnicas e políticas de segurança que protegem as informações pessoais no LGPD que tem seu controle de acesso não autorizado, uso indevido ou divulgação, modificação não autorizada e ilegal destruição ou perda acidental.

Fale conosco

Se você tiver dúvidas ou não sentir que suas preocupações não foram integralmente abordadas nestes Termos e Condições, entre em contato conosco por meio dos contatos indicados em nosso endereço eletrônico, no link Fale Conosco.

Reconhecimento

Após a sua aceitação eletrônica, os termos contidos neste Termos e Condições são considerados efetivos a partir da data dessa aceitação e permanecerão efetivos até 6 (seis) semanas após a conclusão do inquérito.

Por favor, reveja os Termos e Condições e avance para aceitar ou recusar a aceitação.
Você aceita os termos e condições?

Sim ( ) Não ( )
(Em caso de Formulário Eletrônico)
reCAPTCHA

(Caso Use Formulário Eletrônico colocar botão de voltar e avançar)
Voltar Avançar

QUESTIONÁRIO DO DIAGNÓSTICO

BLOCO DE INFORMAÇOES INICIAIS

1. Sua empresa é Registrada no SEBRAE?
( ) Sim
( ) Não

2. Qual o porte da sua empresa?
( ) Microempresa (faturamento até R$ 360.000/ano)
( ) Pequena empresa (faturamento R$ 360.000 até R$ 4.800.000/ano)
( ) Médio Porte (faturamento R$ 4.800.000 até R$ 300.000.000 MM?)
( ) Grande Porte (faturamento maior que R$ 300.000.000)

3. Quantos colaboradores sua empresa emprega?
( ) até 30
( ) de 30 a 100
( ) 100 a 500
( ) acima de 500

4. Qual o seu principal tipo de cliente?
( ) Empresas
( ) Consumidor Final

5. Qual a unidade federativa da sede da sua empresa?

Selecione... (combo)

( ) AC	( ) MA	( ) RJ
( ) AL	( ) MG	( ) RN
( ) AP	( ) MT	( ) RO
( ) AM	( ) MS	( ) RS
( ) BA	( ) PA	( ) SC
( ) CE	( ) PB	( ) SE
( ) DF	( ) PE	( ) SP
( ) ES	( ) PI	( ) TO
( ) GO	( ) PR	

6. Qual o setor da sua empresa? (combo)

( ) Agronegócio
( ) Atacado
( ) Bens de Consumo
( ) Finanças
( ) Indústria
( ) Serviços
( ) Tecnologia
( ) Varejo
( ) Outro

BLOCO DE INFORMAÇOES GERAIS

7. A empresa faz tratamento de dados pessoais? (Pop up – conceito)
( ) Sim
( ) Não

8. A empresa faz o tratamento de dados pessoais sensíveis?
( ) Sim
( ) Não

9. A empresa faz o tratamento de dados pessoais de crianças e adolescentes?
( ) Sim
( ) Não

10. O processo de tratamento de dados pessoais é feito com base na boa-fé e os princípios da LGPD (adequação, finalidade, livre acesso, não discriminação, necessidade, prestação de contas, prevenção, qualidade dos dados, responsabilização segurança, transparência,)?
( ) Sim
( ) Não

11. O processo de tratamento de dados pessoais feito pela empresa inclui automatização de qualquer tomada de decisão (RPA), criação de perfis com base nos dados pessoais transferidos (profiling) ou utilização analítica (analytics)? (de Inteligência Artficial?)
( ) Sim
( ) Não

BLOCO DE TRATAMENTO DE DADOS PESSOAIS

12. O processo de tratamento de dados pessoais realizado pela empresa é fundamentado nas bases legais estipuladas na LGPD?
( ) Sim
( ) Não

13. O Processo de tratamento de dados pessoais de acesso público é baseado na finalidade, boa-fé e o interesse público que justificaram sua disponibilização?
( ) Sim
( ) Não

14. O consentimento para tratamento de dados pessoais é obtido por escrito ou por outro meio que demonstre a manifestação de vontade do titular de dados?
( ) Sim
( ) Não

15. Ao obter o consentimento do titular de dados pessoais a empresa deixa de forma clara, precisa e objetiva as finalidades para as quais os dados serão tratados?
( ) Sim
( ) Não

16. A empresa assegura ao titular de dados pessoais o direito de retirar o consentimento para tratamento de dados quando desejar ?
( ) Sim
( ) Não

17. O acesso a dados pessoais está restrito somente a funcionários autorizados?
( ) Sim
( ) Não

18. A empresa possui um Portal de Privacidade para os titulares de dados pessoais nos quais as informações sobre o tratamento de seus dados são disponibilizadas de forma clara, adequada e ostensiva?
( ) Sim
( ) Não

19. Caso haja alteração na finalidade do tratamento de dado pessoal, a empresa possui um procedimento para informar os titulares dos dados pessoais sobre essa mudança?
( ) Sim
( ) Não

20. A empresa realiza o tratamento de dados pessoais sensíveis de acordo com as bases legais específicas previstas na LGPD?
( ) Sim
( ) Não

21. Os dados pessoais sensíveis tratados pela empresa são compartilhados com terceiros?
( ) Sim
( ) Não

22. A empresa obtém o consentimento específico e destacado de um dos pais ou responsável legal para tratar dados pessoais de crianças?
( ) Sim
( ) Não

23. A empresa condiciona a participação de crianças em jogos, aplicações de internet ou outras atividades ao fornecimento de dados pessoais?
( ) Sim
( ) Não

BLOCO DE CONCLUSÃO DO TRATAMENTO DE DADOS PESSOAIS

24. A empresa possui uma política de eliminação periódica de dados pessoais?
( ) Sim
( ) Não

25. Os dados pessoais são tratados por período indeterminado?
( ) Sim
( ) Não

26. A empresa possui um procedimento para eliminação de dados pessoais?
( ) Sim
( ) Não

27. A empresa possui um procedimento para atender solicitações para eliminar dados pessoais de seus sistemas, se necessário?
( ) Sim
( ) Não

28. A empresa anonimiza os dados pessoais que permanecem em seus sistemas após o término do tratamento?
( ) Sim
( ) Não

BLOCO DE DIREITOS DOS TITULARES

29. A empresa possui um procedimento para atender às solicitações de acesso aos dados pessoais realizadas por titulares?
( ) Sim
( )Não

30. A empresa possui registros de todos os dados pessoais por ela tratados e seus respectivos titulares?
( ) Sim
( )Não

31. A empresa possui procedimento para disponibilização e acesso dos dados pessoais de seus titulares caso venham a ser solicitados em até 15 dias após o requerimento?
( ) Sim
( ) Não

32. Os dados pessoais tratados são acessados por terceiros?
( ) Sim
( ) Não

33. A empresa possui a capacidade de indicar para os titulares de dados pessoais em quais processos existe tomada de decisão gerada pelo tratamento automatizado de dados pessoais?
( ) Sim
( ) Não

BLOCO DE TRANSFERÊNCIA INTERNACIONAL DE DADOS

34. A empresa realiza transferência internacional de dados pessoais?
( ) Sim
( ) Não

35. A empresa realiza transferência internacional de dados pessoais de acordo com as bases legais da LGPD?
( ) Sim
( )Não
( )N/A

36. Os países para os quais a empresa realiza transferência internacional de dados possuem grau de proteção de dados adequado?
( ) Sim
( ) Não
( ) N/A

BLOCO DE DEVERES DO CONTROLADOR E DO OPERADOR

37. A empresa possui Registro das Operações de Tratamento de Dados pessoais), conforme exigido pelo art. 37 da LGPD?
( ) Sim
( ) Não

38. Em caso de atividades de tratamento de dados pessoais que resultem em um alto risco para os titulares de dados, você realiza um Relatório de Impacto à Proteção de Dados pessoais (Data Protection Impact Assessment - DPIA)?
( ) Sim
( ) Não

39. A empresa nomeou um Encarregado de dados (Data Protection Officer - DPO)?
( ) Sim
( ) Não

40. A empresa limita o tratamento de dados pessoais ao tratamento necessário para os fins específicos que justificam a sua coleta?
( ) Sim
( ) Não

BLOCO DE BOAS PRÁTICAS

41. A empresa possui políticas, procedimentos, e medidas protetivas (e.g., controles de acesso, criptografia, modificação de dados, mascaramento de dados) que asseguram a segurança e garantia de conformidade com os regulamentos/leis de privacidade?
( ) Sim
( )Não

42. A empresa possui uma política/procedimento de back-up em relação aos dados pessoais?
( ) Sim
( ) Não

43. A empresa contratou algum serviço de assessoria para implementação da LGPD?
( ) Sim
( ) Não

44. A empresa possui estratégia e mapa (roadmap) de implementação para estar em conformidade com as novas regulamentações?
( ) Sim
( ) Não

45. A empresa possui um programa de governança em privacidade?
( ) Sim
( ) Não

46. Os dados pessoais são armazenados em um local e ambiente seguros?
( ) Sim
( ) Não

47. Existe um processo para atualizar políticas, procedimentos, diretrizes de gerenciamento de riscos, procedimentos de violação, etc. para refletir as atualizações / mudanças das expectativas regulatórias ou mudanças internas no programa de privacidade?
( ) Sim
( ) Não

48. A empresa conduz avaliações de vulnerabilidade e testes de penetração em seus sistemas de tratamento de dados pessoais?
( ) Sim
( ) Não

49. A empresa é certificada em algum padrão ou framework de segurança?
( ) Sim
( ) Não

BLOCO DE RH

50. A empresa promove treinamentos obrigatórios para os funcionários, conscientizando-os sobre a importância e sobre suas responsabilidades em relação à privacidade e proteção de dados pessoais?
( ) Sim
( ) Não

51. Existe um processo formal para revisar e atualizar o treinamento periodicamente?
( ) Sim
( ) Não

52. A empresa oferece orientação aos funcionários de terceiros (prestadores de serviços) a respeito das práticas a serem tomadas em relação à proteção de dados pessoais?
( ) Sim
( ) Não

53. A empresa exige que seus funcionários e prestadores de serviços assinem acordos de confidencialidade e segurança de dados?
( ) Sim
( ) Não

54. A empresa instrui seus funcionários e contratados a limitar o armazenamento de dados pessoais do cliente em dispositivos de armazenamento móvel ao mínimo exigido para fins comerciais?
( ) Sim
( ) Não

55. A empresa possui uma política de revisão regular das permissões de acesso aos dados pessoais que garanta o acesso somente aos funcionários e contratados que precisam ter acesso, bem como um procedimento para prevenir prontamente funcionários e contratados desligados de acesso a dados pessoais?
( ) Sim
( ) Não

(Caso Use Formulário Eletrônico colocar botão de voltar e avançar)
Voltar Avançar

BLOCO DE INCIDENTES DE DADOS PESSOAIS

56. A empresa possui um processo apropriado para notificar os titulares de dados pessoais sobre uma violação de dados, quando aplicável?
( ) Sim
( ) Não

57. A empresa é capaz de detectar rapidamente incidentes de segurança (e.g., incluindo acesso não autorizado, destruição, perda, alteração e violações de dados)?
( ) Sim
( ) Não

58. A empresa possui um procedimento para agir, prontamente, em caso de incidentes de segurança, incluindo notificação aos titulares de dados pessoais afetados?
( ) Sim
( ) Não

59. A empresa pode fornecer uma lista de todas as notificações de privacidade de dados que possui?
( ) Sim
( ) Não

60. Sua empresa já passou por algum incidente de violações de segurança da informação nos últimos dois (2) anos?
( ) Sim
( ) Não

61. Sua empresa está atualmente sujeita a quaisquer ações de execução, investigações ou litígios relacionados à privacidade ou à segurança da informação?
( ) Sim
( ) Não

BLOCO DE GOVERNANÇA

62. Os contratos com terceiros da empresa possuem cláusulas compatíveis com os termos e condições das leis de proteção de dados, em vigor?
( ) Sim
( ) Não

63. Os contratos de trabalho da empresa possuem cláusulas compatíveis com os termos e condições das leis de proteção de dados, em vigor?
( ) Sim
( ) Não

64. A empresa possui cláusulas contratuais de privacidade e proteção de dados em seus contratos em casos de transferência internacional de dados pessoais?
( ) Sim
( ) Não

65. A empresa possui uma metodologia de auditoria prévia de privacidade e proteção de dados para fins de negociação com terceiros?
( ) Sim
( ) Não

66. A empresa possui políticas de privacidade (interna e externa) e boas práticas com relação a proteção de dados pessoais alinhadas com as regras da LGPD?
( ) Sim
( ) Não

67. A empresa possui algum tipo de metodologia para fins de acompanhamento das alterações jurídicas, legais e de jurisprudência relacionadas à LGPD e proteção de dados pessoais no Brasil?
( ) Sim
( ) Não

BLOCO DE FINALIZAÇÃO DO DIAGNÓSTICO

(Em caso de Formulário Eletrônico ACIONAR O BOTAO DE ENVIAR QUESTIONARIO E RECEBER DEVOLUTIVA)

(Caso Use Formulário Eletrônico colocar botão de voltar e avançar)
Voltar Avançar

MODELO – POLÍTICA DE SEGURANÇA

Objetivo

O objetivo de uma Política de Segurança da Informação - PSI é estabelecer princípios e diretrizes para assegurar a confidencialidade, integridade e disponibilidade dos dados e dos sistemas de informação utilizados, garantindo a proteção adequada dos ativos e dos dados.

Tais medidas garantem, também, a identificação, proteção, detecção, resposta e recuperação de eventos em casos de eventual incidente de segurança.

Princípios da Segurança da Informação

O compromisso com o tratamento adequado das informações de clientes e público em geral está fundamentado nos seguintes princípios:

- I. Confidencialidade: garantir que a informação não estará disponível ou divulgada a indivíduos, entidades ou aplicativos sem autorização. Em outras palavras, é a garantia do resguardo das informações dadas pessoalmente em confiança e proteção contra a sua revelação não autorizada.

- II. Integridade: garantir que a informação não seja alterada em seu conteúdo e, portanto, é íntegra, autêntica, procedente e fidedigna.

- III. Disponibilidade: permite que a informação seja utilizada sempre que necessário, estando ao alcance de seus usuários.

Ciclo de Vida da Informação

Para efeito de política, deve ser considerado o seguinte ciclo de vida da informação:

- I. Manuseio: é a etapa onde a informação é criada e manipulada.

- II. Armazenamento: consiste na guarda da informação, seja em um banco de dados, em um papel, em mídia eletrônica interna ou externa, entre outros.

- III. Transporte: ocorre quando a informação é transportada de um local para outro, não importando o meio no qual ela está armazenada.

- IV. Descarte: refere-se à eliminação de documento impresso, eliminação de arquivo eletrônico ou destruição de mídias de armazenamento (por exemplo, CDs, DVDs, disquetes, pen-drives).

Níveis de Acesso aos Dados

O processo de controle de acesso à informação visa garantir que o acesso físico e lógico à informação seja franqueado exclusivamente a pessoas autorizadas, com base nos requisitos de negócio e de segurança da informação.

A organização deve estabelecer em seus contratos, acordos, convênios ou ajustes, cláusulas específicas sobre sigilo, em especial quando informações forem disponibilizadas à terceiros, que assegurem a observância da LGPD.

A definição dos níveis de acesso deve considerar três aspectos:

Quem acessa?
Devem ser definidos os cargos ou as pessoas de determinadas funções que podem acessar os dados. Isso garante que um gestor de RH ou um vendedor sempre tenha acesso ao mesmo número de informações necessário para a execução de suas tarefas diárias.

Como acessa?
Por meio de quais sistemas e dispositivos a pessoa poderá cessar os dados.
Quando acessa?
Fora do horário de expediente ou de sua jornada de trabalho, a pessoa pode consultar os dados?

Controles Internos de Segurança da Informação

1. Identificação/Avaliação de Ameaças e Vulnerabilidades
É a identificação e avaliação dos riscos a que os processos e ativos relevantes estejam sujeitos em virtude das vulnerabilidades e possíveis cenários de ameaça atribuídos a cada processo ou ativo.

Os equipamentos, os sistemas e os aplicativos da organização precisam ser regularmente avaliados e atualizados.

É necessário investir em práticas de segurança para cada componente da infraestrutura.

2. Ações de Prevenção e Proteção

Sem prejuízo de ações específicas para proteção e prevenção de riscos identificados e avaliados, devem ser adotadas rotinas padronizadas de prevenção e proteção dos processos e ativos, realizando análises de vulnerabilidade, testes de intrusão e outras avaliações específicas que certifiquem o cumprimento dos requisitos de segurança e as responsabilidades previamente estabelecidas.

3. Monitoramento e Testes

Devem ser implementados controles internos efetivos para proteção dos Recursos de Tecnologia da Informação e Comunicação, garantindo a sua confidencialidade, integridade, disponibilidade, com as melhores práticas de mercado e regulamentações vigentes.

Os aplicativos críticos devem implementar a geração/manutenção de trilhas de auditoria, controle de versionamento do código fonte e segregação entre os ambientes de produção, homologação e teste. As ameaças cibernéticas devem ser analisadas e devem possuir monitoramento proativo.

4. Plano de Ação e de Resposta a Incidentes

Os incidentes de segurança da informação devem ser identificados e registrados para acompanhamento pelos planos de ação e análise das vulnerabilidades.

Os incidentes deverão ser avaliados e investigados de forma a construir uma análise consistente de causas-consequências, riscos envolvidos, partes envolvidas e planos de respostas. Deverá ser emitido, tempestivamente, comunicado às partes envolvidas informando a situação ocorrida e ações definidas, ainda que preliminares, informando/notificando as atividades posteriores pertinentes.

Um Plano de Ação deverá ser elaborado para implementação das soluções para administração de eventuais contingências e continuidade pós incidente. Tal plano deve contar com definição expressa dos papéis e responsabilidades na solução do impasse. O Plano de Ação deverá, ainda, prever os casos de necessidade de utilização das instalações de contingências nos casos mais severos.

Os Sistemas de Informação, além de disponibilizar os registros em prazos e formatos que atendam às exigências legais, devem protegê-los contra perda, acesso indevido, destruição e falsificação, visando à salvaguarda dos dados.

Sistema de Gestão da Segurança da Informação

Deve-se estabelecer um Sistema de Gestão da Segurança da Informação (SGSI) que é um conjunto de disciplinas, deveres e boas práticas para estabelecer, implementar, operar, monitorar, revisar, manter e aprimorar a segurança da informação visando a coordenação de ações em quatro grandes frentes de atuação:

- I. Governança das políticas e procedimentos de segurança da informação;
- II. Recursos e componentes de segurança da informação;
- III. Monitoramento contínuo do ambiente de tecnologia da informação;
- IV. Gestão de crises e continuidade de negócios.

Elaborando a Política de Segurança

Para definir e implementar uma PSI é importante definir as pessoas ou equipes que vão ser responsáveis pela elaboração, implantação e manutenção da política. Da mesma sorte, definir as responsabilidades de cada equipe/pessoa, trabalhar em conjunto com pessoas da alta administração da organização para aprovação da política e de fato obter maior respeito dos colaboradores que passarão também a conhecer a política.

Devem ser planejados procedimentos apropriados para garantir a conformidade e o respeito às exigências legais quanto à disponibilização de informações, bem como ao uso e disseminação de informações protegidas por leis tais como: dados pessoais, informações relativas à honra e à imagem, de propriedade intelectual, direitos autorais, segredos comerciais, patentes e marcas registradas ou aquelas classificadas como sigilosas.

- Invista em tecnologia: os aplicativos de negócios e sistemas de TIC precisam ser adequados e configurados para garantir a aplicação da Política de Segurança da Informação - PSI, caso contrário, ela cairá em descrédito;

Divulgar e comunicar as definições e conceitos é estratégico para o sucesso da implantação da PSI;
Defina uma agenda de campanha de conscientização dos colaboradores, para relembrá-los o que não deve ocorrer dentro do ambiente interno, de forma a minimizar erros e falhas neste aspecto.

Principais fases para a elaboração de uma política

- I.Identificação dos recursos críticos: mapear os processos da empresa e definir prioridades, importância de cada processo, estabelecendo prioridades de segurança nos processos que mais influenciam na organização;

- II.Classificação das informações: deve-se classificar a importância da informação dentro da organização e assim definir o grau de proteção e as medidas para a sua manipulação, podendo ser confidencial, uso interno e pública;

- III.Elaboração de normas e procedimentos: contemplando os principais aspectos de uso da infraestrutura e dos sistemas de sua organização com foco na segurança.

Política de Privacidade Aderente à LGPD

A política de privacidade objetiva dar visibilidade ao tratamento de dados pessoais em um determinado serviço, atendendo princípios da Lei Geral de Proteção de Dados Pessoais - LGPD.

É importante garantir que a política esteja facilmente disponível. Dessa forma, a organização demonstra profissionalmente seu compromisso com a transparência no tratamento dos dados pessoais. E o usuário deve demonstrar seu expresso consentimento e concordância com os termos da política antes do início desse tratamento.

Para a elaboração da política de privacidade, é fundamental entender o contexto do tratamento de dados pessoais e como os princípios da LGPD são atendidos no sistema ou serviço. Para tanto, é necessário mapear todos os dados pessoais, a finalidade, as bases legais que legitimam o tratamento e a forma de atendimento aos direitos do titular como acesso, retificação, exclusão, revogação de consentimento, oposição, informação sobre possíveis compartilhamentos com terceiros e portabilidade. É fundamental também a definição dos dados, caracterizando-os como públicos, internos, confidenciais e secretos.

Para apoiar o levantamento e a análise das informações, recomenda-se usar o Questionário LGPD (Anexo) para colher e registrar as informações acima. Quaisquer alterações nessas informações devem ser refletidas em versões futuras da política.

Com relação ao conteúdo, é importante observar a presença das seguintes informações, que devem ser levantadas e registradas de modo claro e preciso:

- Informações sobre a organização responsável pelo tratamento;
- Dados pessoais e respectivas finalidades do tratamento, inclusive os dados não informados pelo usuário (exemplo: IP, localização, etc.);
- Base jurídica do tratamento;
- Prazo de retenção dos dados pessoais;
- Informações de contato do encarregado de proteção de dados da organização (Data Protection Officer (DPO)).

A política de privacidade também deve orientar como são atendidos os direitos do titular de dados pessoais, apresentando como ele pode acessar, retificar, solicitar a exclusão de dados, transferir, limitar ou se opor ao tratamento, e retirar o consentimento. Quando aplicáveis, também devem estar presentes as seguintes informações sobre:

- o compartilhamento dos dados com terceiros e qual a finalidade, inclusive redes sociais;
- a transferência internacional de dados e qual a finalidade;
- o tratamento por legítimo interesse;
- o envio de e-mail marketing e como remover o consentimento, quando autorizado inicialmente pelo titular;
- as decisões automatizadas realizadas;
- a proteção de dados de menores de idade;
- a proteção dos dados sensíveis.

Crie Uma Política Preventiva

Instrua os profissionais a agirem de maneira preventiva, a fim de evitar riscos e ataques cibernéticos e a destruição dos documentos.

Entre as boas práticas, estão:

- Não permitir o uso de pen drives;
- Dar preferência ao uso da nuvem como forma de compartilhar os documentos;
- Manter um filtro de spam atualizado;
- Difundir o uso de senhas complexas, que sejam periodicamente trocadas;
- Não acessar a rede Wi-Fi da empresa para atividades particulares no celular.

Estabeleça Níveis de Acesso

Outro fator imprescindível na política de segurança é a criação de níveis de acesso. Isso que garantirá o controle das informações. Algumas informações são restritas e precisam ser preservadas com muito cuidado.

ANEXO - DEVOLUTIVA

Senhor Empresário,
com base nas respostas registradas e na metodologia de avaliação de conformidade com a LGPD, o Diagnóstico de sua organização é de:

- ( ) Não Conformidade
- ( ) Em Conformidade Parcial
- ( ) Em Conformidade

O resultado da apuração percentual de conformidade (XX%) com a LGPD obtido com as respostas registradas, mostra que sua organização precisa empreender um esforço executando, no mínimo, as recomendações abaixo para aumentar o nível conformidade com a essa legislação.

1. Bloco de Tratamento de Dados Pessoais

Se você respondeu sim a pelo menos uma das questões de 7 a 10, tenha certeza de que o tratamento de dados pessoais deve ser realizado, sempre, de acordo com as bases legais previstas na LGPD.

Um comitê deve ser formado para elencar e rever todos os processos da organização, para que possam ser detectados os dados pessoais que estão sendo tratados e onde sua ocorrência está prevista.

Em todos os sistemas que a organização utiliza, será necessário identificar quais atividades de tratamento de dados tais ferramentas apoiam. E depois verificar, periodicamente, por meio de avaliações, qual a base legal pertinente, tempo de retenção dos dados, medidas de segurança, dados pessoais envolvidos, dentre outros.

Algumas perguntas podem orientar:

- Quantos e quais são os dados tratados (mapeamento de dados)
- Que tipos de dados estão sendo tratados?
- Quem é o responsável pelos dados?

- Por que os dados foram coletados?
- Qual a razão legal para continuidade do tratamento dos dados?
- Até quando os dados ficarão na base da organização?

Recomenda-se implementar uma solução de Gerenciamento dos Direitos dos Titulares de Dados, para atender às solicitações destes e da ANPD. Um portal de privacidade (front-end) com uma solução de Gerenciamento dos Direitos dos Titulares de Dados com foco nos clientes da organização, gerenciará todo o fluxo de trabalho da solicitação e deve conter as seguintes funcionalidades:

- Formulário de preenchimento da solicitação, que pode ser apresentado em diversos produtos digitais da organização - recomenda-se a implantação de um processo de obtenção do consentimento do titular a ser utilizado pela organização que seja claro, distinto, que não esteja agrupado com outros acordos ou declarações e que seja ativo (fornecido pelo titular, sem o uso de caixas pré-marcadas);
- Validar a identidade dos titulares de dados;
- Identificar os dados pessoais dentro da organização para realizar a divulgação ao titular de dados, sobre a correção, a exclusão ou portabilidade dos dados pessoais.
- Controlar prazos, atividades e custos da solicitação;
- O portal também deve possuir e divulgar boletins informativos direcionados ao público externo explicando como a organização trata o tema de privacidade e proteção de dados, inclusive a política de privacidade contendo informações sobre direitos dos titulares, demonstrando as boas práticas adotadas para manter a proteção desses dados e os esforços da organização em manter a conformidade com as leis de proteção de dados pessoais.
- Deverá existir aviso de privacidade e proteção de dados em todos os pontos em que os dados pessoais são coletados.
- Recomenda-se desenvolver Modelos de Respostas para solicitações de titulares de dados;
- O tratamento de dados pessoais de crianças e adolescentes deverá ser realizado com o consentimento específico e em destaque, dado por pelo menos por um dos pais ou pelo responsável legal.
- A participação de crianças em jogos, aplicações de internet ou outras atividades afins não podem ser condicionadas pelo Controlador, ao fornecimento de informações pessoais além das estritamente necessárias à atividade.
- Recomenda-se elaborar uma Política de Retenção e Descarte de Dados contendo os princípios de retenção e descarte apropriados de dados pessoais, observando os requisitos legais da LGPD.

- Recomenda-se a contratação de uma consultoria externa para assessorar a organização na análise da atual conformidade (compliance) e a sua manutenção com a LGPD.
- Recomenda-se definir um processo para avaliar se os dados transferidos internacionalmente pela organização estão em conformidade com a LGPD.
- Esse processo deve verificar se essa transferência atende aos requisitos definidos pela lei, tais como:
    - Existência de cláusulas-padrão contratuais com os terceiros;
    - Existência de normas corporativas globais definidas pela organização;
    - Existência de certificados, selos ou códigos de conduta regularmente emitidos e aprovados pela ANPD;
    - Se o titular dos dados forneceu o devido consentimento.
    - Além disso, sugere-se a revisão de contratos já firmados com terceiros onde existe transferência internacional de dados pessoais para que sejam incluídas cláusulas padrão e termos voltados à privacidade e proteção de dados.

2. Bloco de Deveres do Controlador e do Operador

- Recomenda-se que o Controlador e o Operador estejam conscientes que o tratamento dos dados pessoais somente poderá ser realizado nas hipóteses previstas pelo artigo 7° da Lei:
    - Mediante fornecimento de consentimento do titular
    - Para cumprimento de obrigação legal ou regulatória pelo Controlador
    - Pela administração pública, para tratamento e uso compartilhado de dados necessários à execução de políticas públicas
    - Para estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais
    - Quando necessário para execução de contrato ou procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados
    - Para exercício regular de direitos em processo judicial, administrativo ou arbitral
    - Para proteção da vida ou da incolumidade física do titular ou terceiro
    - Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária

    - Quando necessário atender interesses legítimos do Controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam proteção dos dados pessoais
    - Para proteção do crédito
- Recomenda-se que, se solicitado, o Controlador tem o dever de fornecer ao Titular dos Dados Pessoais:

    - Confirmação da existência do tratamento de dados ;
    - Acesso aos dados;
    - Correção de dados incompletos, inexatos ou desatualizados;
    - Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados ilicitamente; Eliminação dos dados pessoais;
    - Revisão das decisões tomadas exclusivamente com base em tratamento automatizado de dados pessoais;
    - Portabilidade dos dados a outro fornecedor de serviço ou produto; Informação das entidades com as quais o Controlador realizou uso compartilhado de dados; Informação sobre a possibilidade de não fornecer o consentimento;
    - Revogação de consentimento;
    - Suporte para reclamação à Autoridade Nacional; Concordância com oposição ao tratamento, se irregular.
    - O tratamento de dados pessoais de crianças e adolescentes deverá ser realizado com o consentimento específico e em destaque dado por pelo menos por um dos pais ou pelo responsável legal.

3. Bloco de Boas Práticas

A adaptação à LGPD é uma jornada que demanda profundas mudanças nos principais pilares de uma organização: tecnologias, processos e pessoas.

Antes de pensar em tecnologias novas, deve-se reformular processos e estabelecer novas diretrizes aos colaboradores e fornecedores. É necessário conhecer a legislação em profundidade e entender como sua organização, seus processos e suas atividades serão impactados pela lei.
A seguir, a organização precisa mapear os seus processos e entender como ocorre o fluxo de dados internamente. É preciso identificar quais tipos de dados são processados, por quem são processados e para que são necessários.

Essa é uma ação que auxilia a garantir maior segurança e privacidade aos clientes e menores riscos para a organização.

Para adequar sua empresa à LGPD, recomenda-se:

- 1. montar um comitê de conformidade (compliance)
- 2. definir o encarregado de dados (DPO)
- 3. avaliar os gaps da empresa em relação à privacidade de dados
- 4. adequar os processos para que estejam em conformidade com a LGPD
- 5. fazer a manutenção da proteção dos dados de forma contínua.

A LGPD exige a elaboração e manutenção de um Registro das Operações de Tratamento de Dados pessoais, que deverá incluir:

- Os nomes e os contatos do Controlador/ Operador e, quando aplicável, de qualquer responsável pelo tratamento em conjunto, dos representantes das entidades e do Encarregado de Dados (DPO);
- A finalidade do processamento dos dados;
- A descrição das categorias dos titulares de dados e das categorias dos dados pessoais;
- As categorias de destinatários a quem os dados pessoais foram ou serão divulgados, incluindo os destinatários estabelecidos em países terceiros ou organizações internacionais;
- Os prazos previstos para a exclusão das diferentes categorias de dados;
- As bases legais estipuladas para tratamento de dados.

Recomenda-se a Implantação da Análise de Impacto à Proteção de Dados (AIPD / DPIA) - O foco da Análise de Impacto à Proteção de Dados (AIPD) é identificar riscos de alto impacto e tomar todas as providências cabíveis para reduzi-los. As AIPD ajudam você a identificar a maneira mais eficaz de cumprir suas obrigações de proteção de dados e atender às expectativas individuais de privacidade.

Recomenda-se definir um processo para Análise de Impacto à Proteção de Dados e realizar periodicamente a Análise de Impacto à Proteção de Dados (AIPD)

É recomendável implementar / adquirir uma solução (sistema) para realização da AIPD de forma sistêmica e centralizada. Essa solução deve ter funcionalidades que permitam o gerenciamento das atividades de proteção de dados, gerenciamento do fluxo de trabalho da AIPD, análise de riscos e lacunas (GAPs) dos fluxos de dados pessoais e registro das atividades de proteção de dados.

Embora a adequação à LGPD não seja limitada apenas a tecnologias, contar com uma boa solução de cibersegurança ajuda a evitar muitos problemas e falhas que são potencialmente perigosas e colocam os dados sob muitos riscos.

Para isso, recomendamos soluções que possam ser integradas entre si e trabalhem juntas para uma proteção completa. Ou seja, desde o firewall até o usuário final, informações são coletadas e trocadas de forma segura, valendo-se de criptografia de ponta a ponta e ações proativas, rápidas e automáticas
para garantir a segurança da rede da empresa.

4. Bloco de Recursos Humanos

- Recomenda-se elaborar um programa de treinamento sobre privacidade e proteção de dados para educar os funcionários sobre a importância da privacidade e proteção de dados pessoais, capacitando-os para realizar os processamentos de dados adequadamente, mitigando os riscos de alguma violação de dados, se acontecer.
- Esse programa pode ter duas fases, de acordo com a sua abordagem: A primeira fase é comum para todos os funcionários e abordará o que são as leis de privacidade e proteção de dados, os seus princípios, os riscos de não estar em conformidade com elas, o que são dados pessoais e sensíveis, bases legais, o que é considerado como processamento de dados, como classificar o dado antes de armazená-lo, como descartá-lo corretamente, o papel e importância do encarregado de dados (DPO) e como reportar uma violação de dados na organização. Esta fase pode ser um treinamento online, disponibilizado para os funcionários via EAD.
- Na segunda fase do programa, o treinamento deverá ser direcionado para cada área de negócio, de acordo com a natureza de relacionamento que elas possuem com os titulares de dados (relacionamento com cliente, financeiro, RH, etc.). Essa fase abordará com mais profundidade a aplicação das bases legais de acordo com os tipos de processamento que a área realiza e terá apresentação de cases específicos conforme a atuação da área, e dever ser preferencialmente presencial para os funcionários de cada área.
- Os treinamentos devem ser reciclados periodicamente de acordo com a política interna da organização ou quando houver mudanças significadas nas leis de privacidade.

5. Bloco de Tratamento de Incidentes de Dados Pessoais

Recomenda-se:

- Estabelecer ou reforçar a estratégia de monitoramento dos dados na organização pode ajudar a reduzir as vulnerabilidades e evitar que terceiros mal intencionados roubem, danifiquem informações sigilosas dos usuários. Além disso, por consequência, os riscos de não conformidade com o LGPD também são mitigados.
- Prevenir incidentes com dados pessoais é uma solução que tem foco maior em assegurar a integridade dos dados e arquivos mais sensíveis e restritos da empresa.
- Já a prevenção contra vazamento de dados é uma solução que foca em barrar acessos indevidos aos sistemas e dados pessoais - tal como usuários, senhas e dados de cartão de crédito - e assim os proteger contra ações maliciosas que visem roubar ou vazar essas informações.

6. Bloco de Governança de Dados

A governança de dados é uma metodologia que tem o propósito de coordenar, orientar e definir regras para a criação, coleta e uso dos dados, visando proteger a propriedade intelectual da empresa e garantir a segurança no armazenamento, monitoramento e geração de dados no ambiente corporativo, para isso:

- Recomenda-se implementar um modelo de governança de dados e designar um Encarregado de Dados (DPO), definindo os papéis e responsabilidades para atender às expectativas regulatórias conforme trazidas pela LGPD. Dentre outras, devem ser geridas atividades como:
    - Elaborar e manter a Avaliação de Impacto na Proteção de Dados (AIPD), quando necessário;
    - Estabelecer a governança de dados e sua manutenção;
    - Estabelecer rotina de treinamentos periódicos sobre a LGPD para funcionários e colaboradores;
    - Criar rotina de acompanhamento de jurisprudências, consultas à ANPD, boas práticas de mercado.
    - Realizar auditorias periódicas internas para análise do nível de conformidade;
- Recomenda-se a contratação de uma consultoria externa para assessorar a organização na análise da atual conformidade (compliance) da organização com a LGPD, indicação dos pontos de melhoria técnica e exigências legais, bem como definição de um plano de ação para implementação das ações necessárias para que a organização esteja e permaneça em conformidade com a LGPD.

Informações e contatos
Sebrae
SGAS 605 – Conj. A – Asa Sul – 70.200-645 – Brasília / DF
0800 570 0800
www.sebrae.com.br

B172c
Balbino, Olívio Fernandes.
Consultoria LGPD para Empresas: Leis e Normas:(manual de orientação para aplicação) /Olívio Fernandes Balbino; Alessandra Vieira (colaboradora). – Brasília: Sebrae, 2020.
54 p. il., color.

ISBN

Lei geral de Proteção Dados. I. SEBRAE II. Título III. Vieira, Alessandra (col)

CDU – 332.1

/sebrae

@sebrae

/tvsebrae

@sebrae

SEBRAE

www.sebrae.com.br
0800 570 0800

ISBN: 978-65-5649-301-5