SINIBREF

ROTEIRO LGPD

PARA INSTITUIÇÕES BENEFICENTES

- Principais Conceitos
- Mapeamento dos Dados
- Segurança dos Dados
- Documentos a serem criados
- Resposta a Incidentes

Sumário

INTRODUÇÃO 4

CONCEITOS IMPORTANTES DA LGPD 5

POR ONDE COMEÇAR? 6

COMO CONSCIENTIZAR A INSTITUIÇÃO E SEUS COLABORADORES DE UMA FORMA EFICIENTE? 8

MAPEANDO DADOS PESSOAIS 9

TUDO COMEÇA PELO RH 10

BOAS PRÁTICAS PARA LGPD NO RH 11

TIPOS DE DADOS PESSOAIS IDENTIFICADOS PELA LGPD 12

TIPOS DE BASE LEGAL IDENTIFICADOS PELA LGPD 13

IDENTIFICANDO AS FONTES DE DADOS 14

EXEMPLOS DE FONTES DE DADOS 15

EXEMPLO DE DOCUMENTO DE INVENTÁRIO DE DADOS PESSOAIS PARA RH .16

EXEMPLO DE PLANILHA DE DADOS PARA IDENTIFICAR OS TIPOS DE DADOS PESSOAIS EM UMA INSTITUIÇÃO BENEFICENTE 18

EXEMPLO DE PLANILHA DE DADOS PARA FAZER O MAPEAMENTO DOS DADOS PESSOAIS EM UMA INSTITUIÇÃO BENEFICENTE 19

DOCUMENTAÇÃO DO FLUXO DE DADOS 20

EXEMPLOS DE DOCUMENTAÇÃO DO FLUXO DE DADOS 21

PLANILHA DE ANÁLISE DE RISCOS 23

EXEMPLO DE PLANILHA DE RISCOS 24

PROCESSO DE SEGURANÇA DA INFORMAÇÃO NAS INSTITUIÇÕES BENEFICENTES 26

EXEMPLO DE DOCUMENTO DE PROCESSO DE SEGURANÇA PARA SER IMPLANTADO NAS INSTITUIÇÕES BENEFICENTES 26

A IMPORTÂNCIA DE COLOCAR CLAUSÚLAS DE LGPDS NOS CONTRATOS COM TERCEIROS 28

EXEMPLO DE CLÁUSULA A COLOCAR NO CONTRATO DOS TERCEIROS. 29

A FUNÇÃO DO DPO 31

COMO PREPARAR UMA RESPOSTA A INCIDENTES DE SEGURANÇA PARA ANP 32

EXEMPLO DE UM DOCUMENTO DE RESPOSTA A ANPD DE INCIDENTE 34

OUTROS DOCUMENTOS IMPORTANTES 36

POLÍTICA DE SEGURANÇA AOS COLABORADORES 36

EXEMPLO DE DOCUMENTO DE POLÍTICA DE SEGURANÇA PARA OS COLABORADORES 37

POLÍTICA DE PRIVACIDADE 39

EXEMPLO DE DOCUMENTO DE POLÍTICA DE PRIVACIDADE 39
TERMO DE CONSENTIMENTO 40
EXEMPLO DE DOCUMENTO DE CONSENTIMENTO 41
EXEMPLO DE REGISTRO DE ATIVIDADES DE TRATAMENTO DE DADOS PESSOAIS 43
RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS (DPIA): 44
EXEMPLO DE RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS (DPIA): 45
POLÍTICA DE RETENÇÃO DE DADOS 49
EXEMPLO DE PLANILHA DE POLÍTICA DE RETENÇÃO DE DADOS 49
EXEMPLO DE DOCUMENTO DE RETENÇÃO DE DADOS 49
DOCUMENTOS FINAIS QUE DEVEM SER CRIADOS E MANTIDOS PELA INSTITUIÇÃO 51
CONCLUSÃO 52
AGRADECIMENTO 53

INTRODUÇÃO

A LGPD (Lei Geral de Proteção de Dados) é uma legislação brasileira que foi promulgada em agosto de 2018 e entrou em vigor em setembro de 2020. Ela estabelece regras e diretrizes para o tratamento de dados pessoais por parte de organizações públicas e privadas.

A lei tem como objetivo principal proteger a privacidade e os direitos dos titulares dos dados, garantindo que suas informações pessoais sejam coletadas, armazenadas, processadas e compartilhadas de forma segura e transparente. A LGPD foi inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia e segue uma abordagem semelhante em relação à proteção de dados pessoais.

Alguns dos principais princípios e direitos estabelecidos pela LGPD incluem:

1. Consentimento: O tratamento dos dados pessoais só pode ocorrer com o consentimento do titular dos dados, de forma livre, informada e inequívoca.

2. Finalidade: Os dados pessoais devem ser coletados para finalidades específicas, claras e legítimas, e não podem ser utilizados para fins diferentes daqueles para os quais foram coletados.

3. Necessidade: A coleta e o tratamento dos dados pessoais devem ser limitados ao mínimo necessário para alcançar a finalidade pretendida.

4. Transparência: As organizações devem fornecer informações claras e acessíveis aos titulares dos dados sobre como seus dados estão sendo tratados.

5. Direitos dos titulares dos dados: A LGPD estabelece uma série de direitos para os titulares dos dados, incluindo o direito de acesso, retificação, exclusão, portabilidade e oposição ao tratamento de seus dados pessoais.

6. Segurança: As organizações são responsáveis por adotar medidas de segurança técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados, perda, destruição, alteração ou qualquer forma de tratamento inadequado ou ilícito.

7. Responsabilização e prestação de contas: As organizações devem ser capazes de demonstrar que estão em conformidade com a LGPD, sendo responsáveis por suas práticas de tratamento de dados pessoais.

O não cumprimento das disposições da LGPD pode resultar em penalidades e sanções, que podem incluir advertências, multas de até 2% do faturamento da organização, limitação do tratamento de dados e até mesmo a proibição total das atividades relacionadas ao tratamento de dados.

CONCEITOS IMPORTANTES DA LGPD

Existem alguns conceitos importantes na LGPD (Lei Geral de Proteção de Dados) que são essenciais para entender a legislação e seu impacto na proteção dos dados pessoais. Aqui estão alguns desses conceitos:

1. Dados Pessoais: Refere-se a qualquer informação relacionada a uma pessoa física identificada ou identificável. Isso inclui informações como nome, endereço, CPF, e-mail, entre outros.

2. Tratamento de Dados: Compreende qualquer operação realizada com dados pessoais, como coleta, armazenamento, uso, compartilhamento, modificação, exclusão, entre outros.

3. Controlador: É a pessoa física ou jurídica, de direito público ou privado, que toma as decisões sobre o tratamento de dados pessoais, definindo as finalidades, os meios e os processos envolvidos. É o responsável por garantir a proteção dos dados pessoais.

4. Operador: É a pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, seguindo suas instruções.

5. Consentimento: Refere-se à manifestação livre, informada e inequívoca do titular dos dados pessoais concordando com o tratamento de seus dados para uma finalidade específica. O consentimento deve ser obtido de forma clara e destacada.

6. Anonimização: É o processo pelo qual os dados pessoais são alterados de forma a não mais identificar ou tornar identificável uma pessoa física. Dados anonimizados não estão sujeitos às regras da LGPD.

7. Encarregado de Proteção de Dados (DPO): É o profissional designado pelo controlador para atuar como ponto de contato entre a instituição e os titulares dos dados, bem como para garantir a conformidade com a LGPD.

8. Titular dos Dados: É a pessoa física a quem os dados pessoais se referem, ou seja, a pessoa a quem os dados pertencem e que tem direitos sobre esses dados.

9. Tratamento de Dados Sensíveis: Refere-se a categorias especiais de dados pessoais que requerem proteção adicional, como informações sobre raça, etnia, religião, opiniões políticas, dados genéticos, entre outros.

10. Incidente de Segurança: É qualquer evento que comprometa a segurança dos dados pessoais, como vazamento, perda, acesso não autorizado, destruição ou alteração dessas informações.

POR ONDE COMEÇAR?

1. Conscientização e Treinamento: Comece criando uma conscientização sobre a LGPD e seus requisitos entre os membros da instituição beneficente. Realize treinamentos para o pessoal, destacando os princípios da LGPD, os direitos dos titulares dos dados e as responsabilidades da organização.`

2. Mapeamento de Dados Pessoais: Realize um inventário completo dos dados pessoais coletados, armazenados e processados pela instituição. Identifique os tipos de dados, a finalidade do tratamento, as bases legais para o processamento e os locais onde os dados são armazenados.

3. Análise de Riscos: Realize uma avaliação de riscos para identificar potenciais vulnerabilidades e ameaças aos dados pessoais. Identifique as possíveis

consequências dos riscos identificados e priorize as áreas que requerem maior atenção e proteção.

4. Revisão das Políticas e Procedimentos: Revise as políticas e procedimentos existentes da instituição para garantir que estejam em conformidade com a LGPD. Crie políticas específicas de privacidade e proteção de dados, estabelecendo diretrizes claras para o tratamento e proteção dos dados pessoais.

5. Implementação de Medidas Técnicas e Organizacionais: Adote medidas técnicas e organizacionais para proteger os dados pessoais. Isso pode incluir o uso de criptografia, o controle de acesso aos dados, a implementação de firewalls e a adoção de práticas de segurança de TI adequadas.

6. Nomeação de um Encarregado de Proteção de Dados (DPO): Designe um profissional responsável por supervisionar a conformidade com a LGPD e atuar como ponto de contato entre a instituição e os titulares dos dados. O DPO também será responsável por lidar com a ANPD e responder a incidentes de segurança.

7. Implementação de Processos de Consentimento: Estabeleça procedimentos claros para obtenção, registro e gestão do consentimento dos titulares dos dados. Certifique-se de que o consentimento seja obtido de forma voluntária, informada e inequívoca, e que possa ser revogado a qualquer momento.

8. Monitoramento e Auditoria: Estabeleça mecanismos para monitorar e auditar regularmente o cumprimento das políticas e procedimentos de proteção de dados. Isso pode incluir revisões internas, auditorias de segurança e testes de conformidade.

9. Revisão dos Contratos com Terceiros: Verifique e atualize os contratos com fornecedores e parceiros que têm acesso aos dados pessoais da instituição. Inclua cláusulas específicas de proteção de dados nos contratos para garantir que os terceiros também estejam em conformidade com a LGPD.

10. Manutenção da Conformidade: A conformidade com a LGPD não é um evento único, mas um processo contínuo. É importante realizar revisões regulares,

atualizar políticas e procedimentos conforme necessário e manter-se atualizado sobre as mudanças na legislação e nas melhores práticas de proteção de dados.

COMO CONSCIENTIZAR A INSTITUIÇÃO E SEUS COLABORADORES DE UMA FORMA EFICIENTE?

1. **Campanha de Comunicação Interna**: Desenvolva uma campanha de comunicação interna para destacar a importância da proteção de dados pessoais e conscientizar os funcionários sobre a LGPD. Isso pode incluir o uso de e-mails, cartazes, murais digitais ou intranet para transmitir mensagens claras e impactantes sobre a LGPD e seus princípios.

Exemplo de mensagem: "Proteja a Privacidade: A LGPD e você. Nossa responsabilidade é proteger os dados pessoais dos nossos beneficiários. Saiba mais sobre a LGPD e como desempenhar um papel ativo na segurança dos dados!"

2. **Sessões de Treinamento:** Realize sessões de treinamento interativas para todos os funcionários da instituição. Essas sessões podem ser conduzidas por especialistas em proteção de dados ou advogados especializados em LGPD. Certifique-se de abordar os conceitos da LGPD, os direitos dos titulares dos dados e as práticas adequadas de tratamento de dados.

Exemplo de atividade: Realize estudos de caso relacionados à instituição beneficente, destacando situações em que a proteção de dados é crucial. Peça aos funcionários para discutir em grupos as ações corretas a serem tomadas para garantir a conformidade com a LGPD.

3. **Materiais Informativos:** Crie materiais informativos para serem distribuídos aos funcionários. Isso pode incluir folhetos, cartilhas ou documentos digitais que expliquem de forma clara e concisa os princípios da LGPD, os direitos dos titulares dos dados e as obrigações da instituição.

Exemplo de tópicos abordados: Princípios da LGPD (finalidade, adequação, necessidade, transparência), direitos dos titulares dos dados (acesso, retificação, exclusão) e responsabilidades da instituição (consentimento, segurança, notificação de incidentes).

4. **Testes de Conhecimento:** Após o treinamento, conduza testes de conhecimento para avaliar a compreensão dos funcionários sobre a LGPD. Isso ajudará a identificar lacunas de conhecimento e áreas que precisam de reforço.

Exemplo de pergunta: "Qual é a diferença entre dados pessoais e dados sensíveis, de acordo com a LGPD?"

5. **Atualizações e Lembretes Regulares:** Mantenha os funcionários atualizados sobre as alterações relevantes na LGPD e envie lembretes regulares sobre as melhores práticas de proteção de dados. Isso pode ser feito por meio de boletins informativos, e-mails ou atualizações na intranet da instituição.

Exemplo de atualização: "Novas orientações da ANPD: Agora é obrigatório obter consentimento explícito para o uso de dados pessoais em campanhas de marketing. Certifique-se de revisar nossos procedimentos para garantir a conformidade."

MAPEANDO DADOS PESSOAIS

Mapear os dados pessoais é um passo importante para implementar a LGPD de forma eficaz em uma associação. O objetivo do mapeamento é identificar quais dados pessoais são coletados, armazenados e processados pela organização, além de compreender como esses dados fluem dentro da instituição. Aqui estão algumas etapas para realizar o mapeamento de dados pessoais:

1. **Identifique os tipos de dados pessoais:** Comece identificando os diferentes tipos de dados pessoais que a associação coleta e processa. Isso pode incluir informações como nome, endereço, número de telefone, endereço de e-mail, informações de pagamento, entre outros.
2. **Identifique as fontes de dados:** Identifique as fontes de onde os dados pessoais são obtidos. Isso pode incluir formulários preenchidos pelos associados, registros de participação em eventos, inscrições em newsletters, interações em redes sociais, entre outros.

3. **Mapeie os processos de tratamento de dados:** Analise como os dados pessoais são coletados, armazenados, processados e compartilhados dentro da associação. Isso pode envolver a identificação de sistemas de armazenamento, bancos de dados, planilhas ou outras ferramentas utilizadas para o tratamento dos dados.

4. **Documente os fluxos de dados:** Visualize e documente como os dados pessoais fluem dentro da associação. Identifique quais departamentos ou setores têm acesso aos dados, como eles são compartilhados internamente e se há compartilhamento com terceiros, como fornecedores ou parceiros.

5. **Avalie as bases legais para o tratamento de dados:** Identifique as bases legais que justificam o tratamento dos dados pessoais pela associação. Isso pode incluir o consentimento do titular, o cumprimento de obrigações contratuais, o cumprimento de obrigações legais, o exercício de direitos em processos judiciais, entre outros.

6. **Registre as informações coletadas:** Documente todas as informações coletadas durante o processo de mapeamento dos dados pessoais. Isso pode ser feito por meio de um inventário ou matriz que contenha informações como o tipo de dado, a finalidade da coleta, a base legal, as fontes de dados, os sistemas utilizados, entre outros detalhes relevantes.

TUDO COMEÇA PELO RH

Com a LGPD em vigor, é importante que os processos de recrutamento sejam aprimorados e simplificados para garantir a conformidade com a legislação de proteção de dados. Aqui estão algumas práticas recomendadas para melhorar o processo de recrutamento de acordo com a LGPD:

1. **Revisão das Políticas e Procedimentos:** Revise e atualize as políticas e procedimentos de recrutamento da instituição beneficente para garantir que estejam alinhados com as diretrizes da LGPD. Isso pode incluir a definição de medidas de segurança para proteger os dados pessoais dos candidatos, a definição de prazos de retenção adequados para os dados coletados durante o processo de recrutamento e a revisão dos consentimentos obtidos.

2. **Minimização de Dados:** Colete apenas os dados pessoais estritamente necessários para o processo de recrutamento. Evite solicitar informações excessivas ou irrelevantes que não sejam relevantes para a seleção dos candidatos. Mantenha o foco nos dados que são relevantes para a avaliação das qualificações e habilidades dos candidatos.

3. **Consentimento Informado:** Obtenha o consentimento informado dos candidatos antes de coletar, processar ou armazenar seus dados pessoais. Informe claramente os propósitos específicos para os quais os dados serão utilizados, bem como os direitos dos candidatos em relação aos seus dados pessoais.

4. **Transparência:** Forneça informações claras e transparentes aos candidatos sobre como seus dados pessoais serão tratados durante o processo de recrutamento. Isso pode incluir a disponibilização de uma política de privacidade, esclarecendo quais dados serão coletados, como serão usados, quem terá acesso a eles e como serão protegidos.

5. **Segurança dos Dados:** Implemente medidas de segurança adequadas para proteger os dados pessoais dos candidatos. Isso pode envolver a adoção de

medidas técnicas e organizacionais para prevenir acesso não autorizado, perda, uso indevido ou divulgação dos dados.

6. **Retenção de Dados:** Estabeleça um prazo de retenção adequado para os dados pessoais dos candidatos. Após o término do processo de recrutamento, revise e atualize regularmente os dados armazenados, garantindo a exclusão dos dados pessoais dos candidatos que não foram selecionados.

7. **Treinamento da Equipe:** Realize treinamentos regulares com a equipe de recrutamento para conscientizá-los sobre as melhores práticas de proteção de dados e as responsabilidades no tratamento dos dados pessoais dos candidatos. Certifique-se de que eles estejam atualizados sobre as diretrizes da LGPD e saibam como implementá-las adequadamente.

8. **Auditoria e Monitoramento:** Realize auditorias regulares para garantir que o processo de recrutamento esteja em conformidade com a LGPD. Monitore continuamente o tratamento de dados pessoais durante o processo de recrutamento e implemente as correções necessárias, caso sejam identificadas não conformidades.

Aprimorar e simplificar o processo de recrutamento de acordo com a LGPD não apenas garantirá a conformidade legal, mas também reforçará a confiança dos candidatos na instituição beneficente, demonstrando o compromisso com a proteção de seus dados pessoais.

BOAS PRÁTICAS PARA LGPD NO RH

1. **Solicite Currículos Digitais:** Incentive os candidatos a enviarem seus currículos em formato digital, preferencialmente por meio de plataformas online seguras ou por e-mail. Isso evita a necessidade de armazenamento de currículos impressos e facilita a organização e o gerenciamento dos dados pessoais.

2. **Utilize um Sistema de Gerenciamento de Candidatos:** Implemente um sistema de gerenciamento de candidatos (ATS - Applicant Tracking System) que permita coletar, armazenar e gerenciar os dados dos candidatos de forma segura e organizada. Esses sistemas podem ajudar a automatizar o processo de recrutamento e garantir a conformidade com a LGPD.

3. **Defina Políticas de Retenção de Dados:** Estabeleça políticas claras de retenção de dados para os currículos recebidos. Determine um prazo adequado para a retenção dos dados dos candidatos e certifique-se de excluí-los de forma segura após esse período, caso não sejam mais relevantes para o processo de recrutamento.

4. **Proteja os Dados Digitais:** Mantenha os dados dos candidatos armazenados em ambientes seguros, com medidas de proteção adequadas, como criptografia e controle de acesso. Utilize soluções de segurança cibernética para proteger os dados contra ameaças externas, como ataques cibernéticos ou vazamentos de informações.

5. **Treine a Equipe de RH:** Capacite a equipe de Recursos Humanos sobre as práticas adequadas de proteção de dados e a importância de evitar o uso de currículos impressos. Certifique-se de que eles estejam familiarizados com as políticas e procedimentos estabelecidos para o tratamento seguro de dados pessoais no processo de recrutamento.

6. **Sensibilização dos Candidatos:** Informe os candidatos sobre as práticas de tratamento de dados adotadas pela instituição beneficente, destacando que os currículos impressos não são utilizados ou armazenados. Incentive-os a enviar seus currículos em formato digital e explique os benefícios em termos de segurança e conformidade com a LGPD.

TIPOS DE DADOS PESSOAIS IDENTIFICADOS PELA LGPD

A LGPD define diferentes tipos de dados pessoais que são protegidos pela legislação. Alguns dos principais tipos de dados pessoais incluem:

1. **Dados de Identificação:** São informações que identificam ou podem identificar uma pessoa física de maneira direta ou indireta. Isso inclui nome, número de identificação (RG, CPF, etc.), data de nascimento, fotografia, entre outros.

2. **Dados de Contato:** São informações que permitem entrar em contato com uma pessoa, como endereço residencial, endereço de e-mail, número de telefone, entre outros.

3. **Dados Sensíveis:** São informações mais sensíveis e que requerem uma proteção especial. Isso inclui dados sobre origem racial ou étnica, convicções religiosas, opiniões políticas, filiação sindical, dados genéticos, dados biométricos, dados de saúde, dados relativos à vida sexual, entre outros.

4. **Dados Financeiros:** São informações relacionadas às finanças e ao histórico financeiro de uma pessoa, como número de conta bancária, informações de cartão de crédito, histórico de transações, entre outros.

5. **Dados Profissionais:** São informações relacionadas ao emprego ou ocupação de uma pessoa, como currículo, histórico de trabalho, informações sobre remuneração, entre outros.

6. **Dados de Localização:** São informações sobre a localização de uma pessoa, como endereço residencial, coordenadas de GPS, dados de geolocalização, entre outros.

TIPOS DE BASE LEGAL IDENTIFICADOS PELA LGPD

A LGPD (Lei Geral de Proteção de Dados) identifica algumas bases legais que podem fundamentar o tratamento de dados pessoais. Essas bases legais estabelecem as condições sob as quais é permitido o tratamento de dados pessoais. Os tipos de base legal identificados pela LGPD são:

1. **Consentimento:** O tratamento de dados pessoais é permitido quando o titular dos dados dá seu consentimento de forma livre, informada e inequívoca. O consentimento deve ser obtido de maneira clara e específica, destacando a finalidade do tratamento.

2. **Execução de contrato:** O tratamento de dados pessoais é permitido quando é necessário para a execução de um contrato do qual o titular dos dados é parte ou para a realização de diligências pré-contratuais.

3. **Cumprimento de obrigação legal ou regulatória:** O tratamento de dados pessoais é permitido quando é necessário para o cumprimento de uma obrigação legal ou regulatória imposta ao controlador dos dados.

4. **Proteção da vida ou da incolumidade física:** O tratamento de dados pessoais é permitido quando é necessário para proteger a vida ou a integridade física do titular dos dados ou de terceiros.

5. **Tutela da saúde:** O tratamento de dados pessoais é permitido quando é necessário para fins de saúde, em procedimentos realizados por profissionais de saúde ou por entidades de saúde.

6. **Legítimo interesse:** O tratamento de dados pessoais é permitido quando o controlador ou terceiro demonstrar um legítimo interesse que justifique o tratamento, desde que esse interesse não viole os direitos e liberdades fundamentais do titular dos dados.

É importante observar que o tratamento de dados pessoais deve ser realizado em conformidade com a base legal adequada e respeitando os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização estabelecidos pela LGPD. Cada situação de tratamento de dados deve ser analisada cuidadosamente para determinar a base legal apropriada para o tratamento.

IDENTIFICANDO AS FONTES DE DADOS

"fonte de dados" refere-se à origem dos dados pessoais que são coletados, utilizados e armazenados pela organização. É o local ou a forma pela qual os dados pessoais são obtidos.

Ao preencher o campo "fonte de dados" em um documento ou registro de tratamento de dados, é necessário identificar de onde os dados foram obtidos. Isso é importante para garantir a transparência e a conformidade com a lei, além de permitir que os titulares dos dados conheçam a origem e a forma como seus dados estão sendo tratados.

Algumas possíveis fontes de dados podem incluir:

1. Titular dos dados: Os dados podem ser fornecidos diretamente pelo próprio titular, por exemplo, por meio de formulários preenchidos, cadastros online, aplicativos, etc.

2. Terceiros: Os dados podem ser obtidos de terceiros, como parceiros de negócios, fornecedores, provedores de serviços, agências de marketing, entre outros, desde que seja garantida a legalidade dessa obtenção.

3. Observação direta: Em certos casos, os dados podem ser obtidos por meio de observação direta, como em sistemas de monitoramento de segurança ou registros de atividades.

4. Fontes públicas: Alguns dados podem ser coletados de fontes públicas acessíveis, como registros públicos, sites, redes sociais, entre outros, desde que seja respeitada a legalidade e a privacidade dos titulares dos dados.

É importante que a organização seja transparente em relação à fonte dos dados pessoais, informando de maneira clara e acessível aos titulares dos dados a origem dessas informações. Além disso, a organização deve ter uma base legal adequada para o tratamento dos dados, independentemente de sua fonte.

EXEMPLOS DE FONTES DE DADOS

Alguns exemplos de fontes de dados que podem ser mencionadas em um documento de LGPD:

1. Cadastro de clientes: Informações pessoais fornecidas pelos clientes durante o processo de cadastro, como nome, endereço, e-mail, número de telefone, CPF, entre outros.

2. Cadastro de funcionários: Dados pessoais dos funcionários da organização, como nome, endereço, data de nascimento, número de registro de funcionário, informações de contato, dados bancários, entre outros.

3. Banco de dados de fornecedores: Informações pessoais dos fornecedores da organização, como nome, endereço, e-mail, número de telefone, CNPJ, informações de contato, entre outros.

4. Dados de marketing: Dados pessoais coletados para fins de marketing, como endereços de e-mail de assinantes de newsletters, dados de clientes para campanhas promocionais, entre outros.

5. Registros de atendimento ao cliente: Dados pessoais coletados durante o atendimento ao cliente, como informações de contato, registros de reclamações ou solicitações, histórico de interações, entre outros.

6. Dados de navegação online: Informações coletadas por meio de cookies ou tecnologias similares em sites ou aplicativos, como endereço IP, informações de geolocalização, preferências de navegação, histórico de páginas visitadas, entre outros.

7. Dados de transações financeiras: Informações pessoais coletadas durante transações financeiras, como dados de cartão de crédito, informações bancárias, histórico de pagamentos, entre outros.

8. Dados de saúde: Informações pessoais relacionadas à saúde dos indivíduos, como prontuários médicos, registros de tratamentos, alergias, entre outros.

9. Dados de recursos humanos: Dados pessoais coletados no âmbito de processos de recrutamento e seleção, como currículos, informações de emprego anterior, referências, entre outros.

10. Dados de monitoramento de atividades: Informações coletadas por meio de sistemas de monitoramento, como registros de acesso a áreas restritas, registros de uso de sistemas e aplicativos internos, entre outros.

EXEMPLO DE DOCUMENTO DE INVENTÁRIO DE DADOS PESSOAIS PARA RH

Inventário de Dados Pessoais - Departamento de Recursos Humanos

Data da criação: [Data]

Responsável pelo inventário: [Nome do Responsável]

1. **Dados de Identificação:**

- Nome completo
- Número de identificação (RG, CPF, etc.)

- Data de nascimento
- Estado civil
- Nacionalidade

2. Dados de Contato:

- Endereço residencial
- Endereço de e-mail
- Número de telefone fixo
- Número de telefone celular

3. Dados Profissionais:

- Currículo vitae
- Histórico de empregos anteriores
- Cargo atual
- Salário e benefícios
- Avaliações de desempenho
- Registros de frequência e horário de trabalho
- Histórico de promoções

4. Dados de Saúde e Segurança:

- Informações sobre saúde física e mental relevantes para a função
- Registros de acidentes de trabalho
- Registros de licenças médicas

5. Dados Financeiros:

- Informações bancárias para depósito de salário
- Dados de pagamento, como folhas de pagamento e comprovantes de pagamento

6. Dados de Treinamento e Desenvolvimento:

- Registros de treinamentos realizados
- Certificados de qualificação profissional

7. Dados de Benefícios e Previdência:

- Informações sobre planos de saúde
- Benefícios adicionais oferecidos
- Informações sobre plano de previdência

8. Dados de Recrutamento e Seleção:

- Currículos e documentos enviados pelos candidatos
- Entrevistas e avaliações dos candidatos
- Registros de referências profissionais

9. Outros Dados:

- Quaisquer outros dados pessoais coletados e tratados pelo departamento de RH

Base Legal para o Tratamento dos Dados Pessoais:

- Fundamento legal para o tratamento dos dados (ex: consentimento, cumprimento de obrigações contratuais, obrigação legal, interesse legítimo, etc.)

Finalidade do Tratamento dos Dados Pessoais:

- Descrição da finalidade para a qual os dados são coletados e tratados pelo departamento de RH

Período de Retenção dos Dados Pessoais:

- Indicação do prazo de retenção dos dados pessoais, de acordo com as obrigações legais e as políticas internas da instituição

NEM TODOS OS DADOS ACIMA PRECISAM SER COLETADOS ISTO É UM EXEMPLO DE ALGUNS DADOS QUE POSSAM SER TRATADOS EM UMA INSTITUIÇÃO BENEFICENTE O IMPORTANTE É SEMPRE TRABAKHAR COM MINIMIZAÇÃO DOS DADOS OU SEJA COLETAR O MÍNIMO DE DADOS POSSÍVEIS MAIS ESSENCIAL PARA O FUNCIONAMENTO DA INSTITUIÇÃO.

EXEMPLO DE PLANILHA DE DADOS PARA IDENTIFICAR OS TIPOS DE DADOS PESSOAIS EM UMA INSTITUIÇÃO BENEFICENTE

Tipo de Dado	Finalidade da Coleta	Base Legal	Fonte de Dados	Sistema de Armazenamento
Nome	Cadastro de associados	Consentimento	Formulário de Inscrição	CRM
Endereço	Envio de correspondências	Cumprimento de obrigações contratuais	Formulário de Inscrição	CRM

Tipo de Dado	Finalidade da Coleta	Base Legal	Fonte de Dados	Sistema de Armazenamento
E-mail	Comunicação de novidades	Consentimento	Formulário de Inscrição	CRM
Número de telefone	Contato para eventos	Consentimento	Formulário de Inscrição	CRM
Data de Nascimento	Verificação de elegibilidade para programas	Obrigação legal	Documento de identificação	Banco de Dados
Informações de pagamento	Processamento de doações	Consentimento	Formulário de Doação	Sistema de Pagamentos

Acima somente um exemplo de uma planilha para que possa mapear os tipos de dados de uma instituição beneficente.

Lembre-se de revisar e adaptar a planilha para refletir os dados pessoais específicos que sua instituição coleta, bem como as finalidades e bases legais para o tratamento desses dados. O objetivo é ter uma visão clara dos tipos de dados pessoais que estão sendo processados e armazenados pela organização.

Além disso, você pode adicionar outras informações relevantes, como datas de consentimento, duração do armazenamento dos dados, controles de segurança implementados e quaisquer detalhes adicionais que ajudem a compreender melhor o fluxo e a gestão dos dados pessoais na instituição beneficente.

Essa planilha pode ser um recurso útil para rastrear e manter um registro dos tipos de dados pessoais em sua instituição, facilitando a conformidade contínua com a LGPD.

EXEMPLO DE PLANILHA DE DADOS PARA FAZER O MAPEAMENTO DOS DADOS PESSOAIS EM UMA INSTITUIÇÃO BENEFICENTE

Planilha para ajudar no mapeamento dos processos de tratamento de dados em uma instituição beneficente:

Processo	Descrição do Processo	Dados Pessoais Envolvidos	Setor Responsável	Sistema de Armazenamento
Cadastro de Associados	Coleta e registro das informações dos associados	Nome, endereço, e-mail, telefone	Departamento de Associados	CRM
Envio de Newsletter	Envio regular de informativos e	Endereço de e-mail	Departamento de	Plataforma de E-mail

Processo	Descrição do Processo	Dados Pessoais Envolvidos	Setor Responsável	Sistema de Armazenamento
	notícias aos associados		Comunicação	
Gestão de Doações	Processamento de doações e emissão de recibos	Nome, endereço, valor da doação	Departamento Financeiro	Sistema de Gestão Financeira
Inscrição em Eventos	Registro e gerenciamento das inscrições para eventos	Nome, e-mail, telefone, informações de pagamento	Departamento de Eventos	Sistema de Inscrição Online
Atendimento a Solicitações	Resposta a solicitações dos associados (ex: acesso aos dados)	Nome, e-mail, informações solicitadas	Departamento de Atendimento	Sistema de Atendimento ao Cliente

Esta é apenas uma demonstração simples de como a planilha pode ser organizada. Você pode personalizá-la conforme as necessidades específicas da sua instituição beneficente, incluindo outras colunas relevantes para o seu contexto.

Certifique-se de revisar e adaptar a planilha para refletir os processos de tratamento de dados específicos da sua instituição, bem como os dados pessoais envolvidos em cada processo. É importante entender como os dados são coletados, armazenados, processados e compartilhados dentro da organização.

DOCUMENTAÇÃO DO FLUXO DE DADOS

A documentação do fluxo de dados nas instituições beneficentes é de extrema importância por diversas razões:

1. Conformidade com a LGPD: Documentar o fluxo de dados ajuda a garantir que a instituição esteja em conformidade com os requisitos da Lei Geral de Proteção de Dados (LGPD) no que diz respeito ao tratamento de dados pessoais. A LGPD exige que as organizações documentem e demonstrem a transparência em relação ao tratamento de dados, incluindo a descrição do fluxo de dados.

2. Identificação de riscos e vulnerabilidades: Ao documentar o fluxo de dados, é possível identificar e avaliar os riscos e vulnerabilidades associados ao tratamento desses dados. Isso permite que a instituição tome medidas adequadas para mitigar esses riscos e proteger os dados pessoais contra acessos não autorizados, perda ou vazamento.

3. Melhoria na gestão de dados: A documentação do fluxo de dados ajuda a instituição a compreender como os dados pessoais estão sendo coletados, processados, armazenados e compartilhados em seus diferentes processos internos. Isso facilita a identificação de oportunidades de melhoria na gestão de dados e no uso eficiente dessas informações.

4. Transparência e prestação de contas: Documentar o fluxo de dados promove a transparência com relação às práticas de tratamento de dados da instituição. Isso demonstra aos titulares dos dados, parceiros, colaboradores e autoridades regulatórias que a instituição está comprometida com a proteção da privacidade e a conformidade com as leis e regulamentos aplicáveis.

5. Facilitação de auditorias e revisões: A documentação do fluxo de dados auxilia em auditorias internas e externas, bem como em revisões de conformidade. Ter um registro claro e detalhado do fluxo de dados permite que a instituição responda prontamente a solicitações de informações e demonstre a conformidade com as obrigações legais e regulatórias.

Em resumo, a documentação do fluxo de dados é essencial para garantir a conformidade legal, proteger a privacidade dos indivíduos e promover uma gestão adequada e segura dos dados pessoais nas instituições beneficentes.

EXEMPLOS DE DOCUMENTAÇÃO DO FLUXO DE DADOS

Documento de Documentação dos Fluxos de Dados Pessoais

1. Introdução:

Este documento tem como objetivo documentar os fluxos de dados pessoais dentro da instituição beneficente XYZ. Ele visa fornecer uma visão geral dos processos e sistemas envolvidos na coleta, armazenamento, processamento e compartilhamento de dados pessoais.

2. Identificação da Instituição Beneficente:

Nome da instituição: [Nome da instituição beneficente]

Responsável pelo documento: [Nome do responsável]

Data de criação: [Data de criação]

3. Descrição dos Fluxos de Dados:

A seguir, estão os fluxos de dados pessoais identificados dentro da instituição beneficente:

Fluxo de Dados 1: Cadastro de Associados

- Descrição: Esse fluxo de dados envolve o cadastro de associados na instituição beneficente, permitindo a coleta de informações para fins de comunicação e gestão de relacionamento.
- Dados Pessoais Envolvidos: Nome, endereço, e-mail, telefone.
- Setor Responsável: Departamento de Associados.
- Sistema de Armazenamento: CRM (Customer Relationship Management).

Fluxo de Dados 2: Envio de Newsletter

- Descrição: Esse fluxo de dados envolve o envio regular de informativos e notícias aos associados por meio de newsletters eletrônicas.
- Dados Pessoais Envolvidos: Endereço de e-mail.
- Setor Responsável: Departamento de Comunicação.
- Sistema de Armazenamento: Plataforma de E-mail.

Fluxo de Dados 3: Gestão de Doações

- Descrição: Esse fluxo de dados envolve o processamento de doações recebidas pela instituição beneficente, incluindo a emissão de recibos para os doadores.
- Dados Pessoais Envolvidos: Nome, endereço, valor da doação.
- Setor Responsável: Departamento Financeiro.
- Sistema de Armazenamento: Sistema de Gestão Financeira.

Fluxo de Dados 4: Inscrição em Eventos

- Descrição: Esse fluxo de dados envolve o registro e gerenciamento das inscrições dos associados em eventos organizados pela instituição beneficente.
- Dados Pessoais Envolvidos: Nome, e-mail, telefone, informações de pagamento.
- Setor Responsável: Departamento de Eventos.
- Sistema de Armazenamento: Sistema de Inscrição Online.

Fluxo de Dados 5: Atendimento a Solicitações

- Descrição: Esse fluxo de dados envolve o atendimento a solicitações dos associados, como solicitações de acesso aos seus dados pessoais ou outras informações relacionadas.
- Dados Pessoais Envolvidos: Nome, e-mail, informações solicitadas.
- Setor Responsável: Departamento de Atendimento.
- Sistema de Armazenamento: Sistema de Atendimento ao Cliente.

4. Considerações Finais:

Este documento oferece uma visão geral dos fluxos de dados pessoais identificados na instituição beneficente XYZ. É importante revisar e atualizar este documento regularmente, à medida que novos fluxos de dados são implementados ou alterações ocorrem nos processos.

PLANILHA DE ANÁLISE DE RISCOS

A planilha de análise de riscos desempenha um papel fundamental na gestão da privacidade e proteção de dados nas instituições beneficentes, oferecendo várias vantagens e importâncias, como:

1. Identificação de riscos: Através da planilha de análise de riscos, é possível identificar e listar os potenciais riscos relacionados à privacidade e proteção de dados na instituição. Isso inclui ameaças internas e externas que podem comprometer a segurança dos dados pessoais.

2. Avaliação de impacto: A planilha permite avaliar o impacto desses riscos na organização. Isso ajuda a compreender quais riscos são mais significativos e podem causar danos significativos aos dados pessoais, à reputação da instituição ou ao cumprimento das obrigações legais.

3. Priorização de ações: Com base na análise de riscos, a planilha auxilia na priorização de ações para mitigar os riscos identificados. Ela ajuda a definir quais medidas de segurança e proteção devem ser implementadas primeiro, com base na sua gravidade e probabilidade de ocorrência.

4. Tomada de decisões informadas: Ao ter uma visão clara dos riscos e suas consequências, a instituição pode tomar decisões informadas sobre investimentos em segurança da informação, alocação de recursos e implementação de controles apropriados.

5. Monitoramento contínuo: A planilha de análise de riscos permite que a instituição acompanhe e monitore regularmente os riscos identificados. Ela pode ser atualizada conforme novos riscos surgem ou conforme mudanças ocorrem nos processos de tratamento de dados.

6. Conformidade regulatória: A análise de riscos auxilia na identificação dos requisitos de conformidade legal e regulatória, como os estabelecidos pela LGPD. Isso ajuda a garantir que a instituição esteja em conformidade com as leis de proteção de dados aplicáveis e possa fornecer evidências documentadas de suas práticas de segurança e privacidade.

7. Demonstração de responsabilidade: A planilha de análise de riscos é uma forma de demonstrar a responsabilidade da instituição na proteção dos dados pessoais. Ela fornece um registro documentado das ações tomadas para gerenciar os riscos e proteger a privacidade dos dados.

Em resumo, a planilha de análise de riscos é uma ferramenta valiosa para identificar, avaliar e gerenciar os riscos relacionados à privacidade e proteção de dados nas instituições beneficentes. Ela contribui para uma abordagem pró-ativa na gestão da segurança da informação e ajuda a garantir a conformidade com as leis e regulamentos de proteção de dados.

EXEMPLO DE PLANILHA DE RISCOS

Planilha de Análise de Riscos

Ativo	Ameaça	Vulnerabilidade	Impacto	Probabilidade	Risco	Controles de Mitigação
Sistema de Armazenamento de Dados	Acesso não autorizado	Falta de controles de autenticação e autorização	Roubo ou uso indevido de dados pessoais	Média	Alto	Implementação de autenticação de dois fatores, restrição de acesso baseada em função
Dispositivos Móveis	Perda ou roubo	Falta de criptografia de dados	Divulgação de dados pessoais confidenciais	Baixa	Médio	Criptografia de dispositivos móveis, política de senhas fortes
Servidores de Rede	Ataques cibernéticos	Falhas na segurança da rede	Integridade comprometida dos dados pessoais	Alta	Alto	Implementação de firewalls, atualização regular de sistemas e aplicativos
Backup de Dados	Falha no processo de backup	Falta de backups regulares e testes de recuperação	Perda irreversível de dados pessoais	Baixa	Médio	Estabelecimento de políticas de backup e recuperação, testes regulares
Comunicação de Dados	Intercepção de dados durante a transmissão	Falta de criptografia de dados em trânsito	Divulgação não autorizada de informações	Média	Alto	Implementação de protocolos de criptografia (ex: HTTPS)

Ativo	Ameaça	Vulnerabilidade	Impacto	Probabilidade	Risco	Controles de Mitigação
			pessoais			

Na planilha acima, os seguintes elementos são considerados:

- Ativo: Os ativos são os componentes da instituição que envolvem dados pessoais, como sistemas de armazenamento, dispositivos móveis, servidores de rede, backup de dados e comunicação de dados.

- Ameaça: Representa as possíveis ameaças que podem afetar a segurança dos ativos e dos dados pessoais, como acesso não autorizado, perda ou roubo, ataques cibernéticos e intercepção de dados.

- Vulnerabilidade: São as fragilidades nos sistemas e processos que podem ser exploradas pelas ameaças, como falta de controles de autenticação, falhas na segurança da rede e falta de criptografia.

- Impacto: Indica as consequências que podem ocorrer caso uma ameaça seja bem-sucedida, como divulgação de dados pessoais, comprometimento da integridade dos dados e perda irreversível de informações.

- Probabilidade: Representa a probabilidade de uma ameaça se concretizar, podendo ser alta, média ou baixa.

- Risco: Calcula-se o risco multiplicando a probabilidade pelo impacto, fornecendo uma classificação do risco (alto, médio ou baixo).

- Controles de Mitigação: São as medidas de segurança que podem ser implementadas para reduzir ou mitigar os riscos identificados, como autenticação de dois fatores, criptografia, firewalls, políticas de backup e recuperação, entre outros.

Lembre-se de adaptar essa planilha de acordo com as necessidades e particularidades da sua instituição beneficente.

PROCESSO DE SEGURANÇA DA INFORMAÇÃO NAS INSTITUIÇÕES BENEFICENTES

o processo ou política de segurança de informações é essencial para proteger os dados e informações sensíveis da instituição beneficente, garantir a conformidade com as regulamentações aplicáveis, prevenir incidentes de segurança, mitigar riscos e demonstrar responsabilidade na proteção dos dados. É uma parte fundamental da gestão eficaz da segurança da informação.

Uma violação de dados ou incidente de segurança pode ter um impacto significativo na reputação da instituição. Uma política de segurança de informações robusta demonstra o comprometimento da instituição em proteger os dados e pode contribuir para a construção da confiança com os stakeholders.

Stakeholders são pessoas ou grupos que têm interesse, influência ou são afetados pelas atividades e decisões de uma organização. Eles podem ser internos ou externos à instituição beneficente e desempenham um papel importante no seu sucesso e impacto. Ex: Colaboradores, parceiros, doadores, fornecedores etc.

EXEMPLO DE DOCUMENTO DE PROCESSO DE SEGURANÇA PARA SER IMPLANTADO NAS INSTITUIÇÕES BENEFICENTES

Documento de Processo de Segurança das Informações nos Sistemas

1. Introdução:

Este documento tem como objetivo apresentar o processo de segurança das informações nos sistemas da instituição beneficente XYZ. Ele destaca as medidas e práticas adotadas para proteger os dados pessoais e garantir a confidencialidade, integridade e disponibilidade das informações.

2. Identificação da Instituição Beneficente:

Nome da instituição: [Nome da instituição beneficente] Responsável pelo documento: [Nome do responsável] Data de criação: [Data de criação]

3. Políticas de Segurança da Informação:

A instituição beneficente XYZ tem as seguintes políticas de segurança da informação em vigor:

- Política de Acesso aos Sistemas: Define os requisitos de autenticação, autorização e controle de acesso aos sistemas utilizados pela instituição. Inclui o uso de senhas fortes, autenticação de dois fatores e restrições de acesso baseadas em função.

- Política de Classificação de Informações: Estabelece a classificação dos dados pessoais e outras informações em categorias, como confidenciais, internas ou públicas. Define as medidas de segurança apropriadas para cada categoria.

- Política de Backup e Recuperação: Define as práticas de backup regular dos dados e a implementação de procedimentos de recuperação de dados em caso de falha de sistemas ou incidentes de segurança.
- Política de Segurança de Redes: Estabelece as medidas de segurança para proteger a infraestrutura de rede da instituição, como firewalls, detecção de intrusões e monitoramento de tráfego.

4. Medidas de Segurança Técnica:

A instituição beneficente XYZ implementa as seguintes medidas de segurança técnica em seus sistemas:

- Atualização de Software: Mantém os sistemas operacionais, aplicativos e outros softwares utilizados atualizados com as correções de segurança mais recentes.

- Criptografia de Dados: Utiliza criptografia para proteger dados pessoais em trânsito e em repouso, incluindo o uso de protocolos seguros (como HTTPS) e armazenamento criptografado.

- Monitoramento de Segurança: Implementa ferramentas de monitoramento e detecção de atividades suspeitas nos sistemas, com alertas em tempo real e registros de eventos para análise posterior.

- Controles de Acesso: Aplica controles de acesso granulares para restringir o acesso a dados pessoais apenas às pessoas autorizadas, com base em funções e necessidade de conhecimento.

5. Conscientização e Treinamento:

A instituição beneficente XYZ realiza treinamentos periódicos de conscientização em segurança da informação para seus funcionários, destacando a importância da proteção dos dados pessoais e boas práticas de segurança, como a detecção de phishing e o manuseio adequado de informações confidenciais.

6. Auditoria e Revisão:

A instituição beneficente XYZ realiza auditorias regulares dos sistemas e processos de segurança da informação para garantir sua eficácia e conformidade com as políticas estabelecidas. As revisões são conduzidas internamente ou por terceiros independentes.

7. Considerações Finais:

Este documento oferece uma visão geral do processo de segurança das informações nos sistemas da instituição beneficente XYZ. É fundamental revisar e atualizar este documento periodicamente para refletir as mudanças nos sistemas, tecnologias e requisitos de segurança, garantindo a proteção contínua dos dados pessoais e a conformidade com as regulamentações aplicáveis.

Lembre-se de personalizar este documento de acordo com as políticas e práticas específicas da sua instituição beneficente, bem como as regulamentações de segurança e privacidade relevantes em vigor.

A IMPORTÂNCIA DE COLOCAR CLAUSÚLAS DE LGPDS NOS CONTRATOS COM TERCEIROS

A inclusão de cláusulas de LGPD (Lei Geral de Proteção de Dados) nos contratos com terceiros é de extrema importância para garantir a conformidade com a legislação de proteção de dados e proteger os direitos dos titulares dos dados. Algumas razões que destacam a importância dessa prática são:

1. Transferência de responsabilidade: Ao incluir cláusulas de LGPD nos contratos, a instituição beneficente está transferindo a responsabilidade aos terceiros para garantir que eles também estejam em conformidade com as disposições da lei. Isso significa que o terceiro será igualmente responsável pela proteção adequada dos dados pessoais.

2. Proteção dos direitos dos titulares de dados: As cláusulas de LGPD nos contratos com terceiros ajudam a garantir que os direitos dos titulares de dados sejam respeitados. Isso inclui o direito à privacidade, ao acesso, à retificação, à exclusão e à portabilidade dos dados pessoais.

3. Medidas de segurança adequadas: As cláusulas de LGPD podem exigir que os terceiros implementem medidas de segurança adequadas para proteger os dados pessoais. Isso inclui controles de acesso, criptografia, monitoramento de atividades suspeitas, entre outros.

4. Restrições ao uso dos dados: As cláusulas de LGPD podem estabelecer limitações claras quanto ao uso dos dados pessoais pelos terceiros. Isso inclui restrições quanto à finalidade do processamento, a proibição de compartilhamento com outras entidades sem consentimento prévio, entre outros aspectos relevantes.

5. Confidencialidade e sigilo: As cláusulas de LGPD podem incluir disposições de confidencialidade e sigilo, protegendo os dados pessoais contra acesso não autorizado ou divulgação indevida.

6. Auditoria e monitoramento: As cláusulas de LGPD podem permitir que a instituição beneficente realize auditorias e monitoramento das práticas de proteção de dados do terceiro para garantir o cumprimento das obrigações contratuais e legais.

7. Responsabilidade e indenização: As cláusulas de LGPD podem estabelecer a responsabilidade dos terceiros em caso de violação de dados pessoais e definir as medidas de reparação ou indenização em caso de danos causados pela não conformidade.

Em resumo, a inclusão de cláusulas de LGPD nos contratos com terceiros é uma prática essencial para garantir a conformidade legal, proteger os direitos dos titulares de dados e estabelecer medidas de segurança adequadas para a proteção dos dados pessoais. Isso contribui para a construção de relacionamentos confiáveis e para o fortalecimento da cultura de proteção de dados nas instituições beneficentes.

EXEMPLO DE CLÁUSULA A COLOCAR NO CONTRATO DOS TERCEIROS.

Lembrando que é apenas um exemplo o ideal é procurar um advogado para criação e validação da mesma.

Cláusula de Exemplo de LGPD para Inclusão nos Contratos com Terceiros:

"Ao celebrar este contrato, as partes reconhecem e concordam em cumprir com as disposições da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, e comprometem-se a tomar todas as medidas necessárias para garantir a proteção adequada dos dados pessoais compartilhados ou acessados durante a execução deste contrato.

1. Responsabilidades do Controlador:

   1.1. O [Nome da Instituição Beneficente], denominado como Controlador dos dados pessoais, deverá fornecer aos Terceiros as informações necessárias para o cumprimento das obrigações previstas na LGPD.

   1.2. O Controlador deverá obter o consentimento expresso e específico dos titulares dos dados, quando necessário, e manter registros adequados dessa obtenção.

   1.3. O Controlador deverá garantir que os dados pessoais compartilhados com os Terceiros sejam fornecidos apenas na medida necessária para a execução deste contrato, mantendo a confidencialidade e integridade desses dados.

2. Responsabilidades do Operador:

   2.1. O Terceiro, atuando como Operador dos dados pessoais, compromete-se a tratar os dados pessoais somente de acordo com as instruções fornecidas pelo Controlador e em conformidade com a LGPD.

   2.2. O Operador deverá adotar medidas de segurança técnicas e organizacionais apropriadas para proteger os dados pessoais contra perda, acesso não autorizado, destruição, divulgação ou qualquer forma de processamento ilícito.

   2.3. O Operador deverá notificar imediatamente o Controlador caso identifique qualquer violação de segurança ou incidente relacionado aos dados pessoais, tomando as medidas corretivas necessárias.

3. Transferência Internacional de Dados:

   3.1. Caso haja transferência internacional de dados pessoais para países sem um nível adequado de proteção de dados, o Operador deverá adotar mecanismos de garantia de proteção, conforme exigido pela LGPD.

4. Subcontratantes:

   4.1. O Operador somente poderá envolver subcontratantes para o processamento dos dados pessoais com o consentimento prévio e específico do Controlador, e mediante a assinatura de um contrato que estabeleça as mesmas obrigações de proteção de dados previstas neste instrumento.

5. Prazo de Retenção:

5.1. O Operador deverá reter os dados pessoais pelo tempo estritamente necessário para a execução deste contrato, de acordo com as orientações do Controlador e as obrigações legais aplicáveis.

6. Encerramento ou Rescisão do Contrato:

   6.1. Na hipótese de encerramento ou rescisão deste contrato, o Operador deverá, a critério do Controlador, devolver ou excluir os dados pessoais processados durante a vigência deste contrato, de acordo com as orientações recebidas.

7. Disposições Gerais:

   7.1. Este contrato deverá ser interpretado e regido de acordo com a legislação brasileira e qualquer disputa decorrente ou relacionada a este contrato será submetida à jurisdição exclusiva dos tribunais competentes

A FUNÇÃO DO DPO

Primeiramente crie um e-mail para a instituição para centralizar as demandas dos titulares ex: dpo@suainstituicao.com.br (o final pode ser .org .com conforme seu dominio) e defina quem será o DPO da instituição.

A função de um Encarregado de Proteção de Dados (DPO - Data Protection Officer) é desempenhar um papel fundamental na proteção de dados e garantir a conformidade com a LGPD (Lei Geral de Proteção de Dados) e outras leis de privacidade de dados. O DPO tem a responsabilidade de promover e supervisionar a aplicação das práticas de proteção de dados pessoais dentro da organização. Suas funções detalhadas incluem:

1. Monitoramento da conformidade com a LGPD: O DPO é responsável por garantir que a organização esteja em conformidade com os requisitos da LGPD. Isso envolve a revisão das políticas, processos e práticas internas para garantir que eles atendam aos princípios e obrigações estabelecidos na lei.

2. Assessoria e Consultoria: O DPO fornece orientação e aconselhamento interno sobre questões relacionadas à proteção de dados pessoais. Ele oferece suporte aos funcionários da organização, esclarece dúvidas e fornece diretrizes sobre o tratamento adequado dos dados pessoais.

3. Treinamento e Conscientização: O DPO desenvolve e conduz treinamentos internos sobre proteção de dados e a importância do cumprimento das políticas e procedimentos estabelecidos. Ele promove a conscientização sobre os direitos dos titulares dos dados e a importância da privacidade.

4. Avaliação de Impacto de Proteção de Dados (AIPD): O DPO é responsável por realizar a AIPD, que consiste em avaliar os riscos e impactos à privacidade decorrentes das atividades de tratamento de dados. Ele identifica possíveis riscos, recomenda medidas de mitigação e garante que a organização realize a análise e documentação necessárias.

5. Relacionamento com Autoridade de Proteção de Dados: O DPO atua como ponto de contato entre a organização e a Autoridade Nacional de Proteção de Dados (ANPD), que é responsável pela fiscalização e aplicação da LGPD. Ele lida com questões relacionadas a notificações de violações de dados e outros assuntos de interesse da ANPD.

6. Resposta a Incidentes de Segurança: Em caso de violação de dados ou incidente de segurança, o DPO coordena a resposta da organização. Ele avalia o impacto do incidente, notifica as partes relevantes, implementa medidas corretivas e acompanha as ações necessárias para resolver a situação.

7. Atuação como Canal de Comunicação: O DPO serve como canal de comunicação entre a organização, os funcionários e os titulares dos dados. Ele recebe e responde às solicitações, reclamações ou dúvidas relacionadas à proteção de dados pessoais.

É importante ressaltar que a função do DPO varia dependendo do tamanho e da natureza da organização, mas seu principal objetivo é garantir que a privacidade e a proteção dos dados pessoais sejam tratadas de forma adequada e em conformidade com a legislação aplicável.

COMO PREPARAR UMA RESPOSTA A INCIDENTES DE SEGURANÇA PARA ANPD

A resposta a incidentes de segurança é uma ação crucial para lidar com violações de dados e garantir a proteção das informações na organização. Embora os passos específicos possam variar dependendo da situação e dos protocolos internos da ANPD (Autoridade Nacional de Proteção de Dados), aqui está um exemplo geral de um processo passo a passo para responder a um incidente de segurança:

1. Identificação e classificação do incidente: Assim que um incidente de segurança for detectado, ele deve ser prontamente identificado e classificado. Isso envolve entender a natureza do incidente, sua gravidade e impacto potencial nas informações e sistemas .

2. Notificação da equipe responsável: A equipe de resposta a incidentes de segurança da ANPD deve ser notificada imediatamente sobre o incidente.

3. Isolamento e contenção: A equipe de resposta deve tomar medidas para isolar e conter o incidente, evitando que se espalhe para outros sistemas ou afete ainda mais os dados. Isso pode incluir a desconexão de sistemas comprometidos, bloqueio de contas de usuário comprometidas ou isolamento de áreas afetadas.

4. Coleta de evidências: É fundamental coletar e preservar evidências relacionadas ao incidente. Isso pode envolver a captura de registros de logs, informações de atividade do sistema, screenshots, entre outros dados relevantes que possam ajudar na investigação e na análise forense.

5. Análise e investigação: A equipe de resposta a incidentes deve realizar uma análise detalhada para entender a origem e a extensão do incidente. Isso pode envolver a identificação de vetores de ataque, avaliação de sistemas comprometidos, revisão de logs de atividades e outras técnicas de investigação forense.

6. Comunicação interna e externa: Durante o processo de resposta, é importante manter uma comunicação clara e efetiva com as partes envolvidas. Isso inclui a comunicação com a equipe interna , os responsáveis pelo incidente, a alta administração, as autoridades reguladoras relevantes e, se necessário, os afetados pelo incidente.

7. Notificação de autoridades e titulares dos dados: Se o incidente envolver dados pessoais ou informações confidenciais, a DPO deve seguir os procedimentos adequados de notificação às autoridades competentes, e, se necessário, aos titulares dos dados afetados.

8. Mitigação e recuperação: Após a análise do incidente, a equipe de resposta deve desenvolver e implementar medidas de mitigação e recuperação. Isso pode incluir a correção de falhas de segurança, fortalecimento de controles de acesso, implementação de patches de segurança, entre outras ações para evitar futuros incidentes semelhantes.

9. Avaliação pós-incidente e lições aprendidas: Após a resolução do incidente, é importante conduzir uma avaliação pós-incidente para identificar áreas de melhoria e lições aprendidas. Isso pode incluir a revisão de políticas, procedimentos e controles de segurança, além de treinamentos adicionais para a equipe.

10. Monitoramento contínuo e revisão de medidas de segurança: A segurança da informação é um processo contínuo. Após a resposta ao incidente, é essencial monitorar continuamente a infraestrutura, revisar as medidas de segurança existentes e realizar atualizações conforme necessário para garantir a proteção adequada das informações.

EXEMPLO DE UM DOCUMENTO DE RESPOSTA A ANPD DE INCIDENTE

[Logotipo da INSTITUICAO]

Documento de Resposta a Incidente de Segurança

Data: [Data do incidente] Referência: [Número ou identificador do incidente]

1. Detalhes do Incidente:

   a) Data e hora de detecção do incidente:

   b) Descrição do incidente:

   c) Classificação do incidente (por exemplo: violação de dados, malware, acesso não autorizado, etc.):

   d) Gravidade do incidente (alta, média, baixa):

   e) Impacto inicial identificado:

   f) Sistema ou recurso afetado:

   g) Identificação das informações comprometidas:

2. Ação Imediata:

   a) Equipe responsável pelo incidente:

   b) Ações tomadas para isolar e conter o incidente:

   c) Desconexão de sistemas afetados:

   d) Bloqueio de contas de usuário comprometidas:

   e) Outras medidas de segurança implementadas:

3. Análise e Investigação:

   a) Identificação de vetores de ataque:

   b) Revisão de logs de atividade e registros de sistema:

   c) Coleta de evidências:

   d) Análise forense realizada:

   e) Identificação de sistemas ou vulnerabilidades comprometidas:

   f) Avaliação do escopo do incidente:

4. Comunicação:

   a) Comunicação interna:

      - Equipe interna de resposta a incidentes notificada:
      - Contato com a alta administração:
      - Reuniões ou atualizações periódicas para as partes interessadas internas:

   b) Comunicação externa:

      - Notificação às autoridades competentes (ANPD, outros órgãos reguladores):
      - Comunicação aos titulares de dados afetados, quando necessário:
      - Contato com fornecedores, parceiros ou outras partes externas envolvidas:

5. Mitigação e Recuperação:

   a) Medidas de mitigação implementadas:

   b) Correção de falhas de segurança:

   c) Reforço de controles de acesso:

d) Implementação de patches de segurança:

e) Outras ações de recuperação realizadas:

6. Lições Aprendidas:

a) Avaliação pós-incidente realizada:
b) Identificação das áreas de melhoria:
c) Atualização de políticas, procedimentos ou controles de segurança:
d) Necessidade de treinamentos adicionais:

7. Monitoramento e Revisão:

a) Monitoramento contínuo de sistemas e infraestrutura:

b) Revisão periódica das medidas de segurança:

c) Atualizações conforme necessário para evitar futuros incidentes:

Este documento de Resposta a Incidente de Segurança é confidencial e deve ser tratado de forma adequada. Ele fornece um registro das ações tomadas durante o incidente de segurança e serve como um guia para futuras referências e melhorias na segurança da informação.

Assinatura: _____

Nome:_____

Cargo:_____

Data: _____

[Logotipo da INSTITUICAO]

OUTROS DOCUMENTOS IMPORTANTES

POLÍTICA DE SEGURANÇA AOS COLABORADORES

Não adianta de nada se todas as medidas da instituição não tiver colaboração da organização como um todo. Neste sentido é importante além dos treinamentos criar-se o documento de política de segurança para os colaboradores da instituição beneficente a fim de que os mesmo sigam a riscas todas as regras impostas neste documento que deve ser atualizado constantemente.

EXEMPLO DE DOCUMENTO DE POLÍTICA DE SEGURANÇA PARA OS COLABORADORES

Política de Segurança para os Colaboradores

1. Introdução A segurança da informação é de extrema importância para a nossa organização. Todos os colaboradores desempenham um papel fundamental na proteção dos nossos dados e informações confidenciais. Esta política estabelece as diretrizes e responsabilidades para garantir a segurança da informação e evitar incidentes de segurança.
2. Responsabilidades

    2.1. Colaboradores

    - Cumprir as políticas e procedimentos de segurança da informação estabelecidos pela organização.
    - Proteger adequadamente as informações confidenciais às quais têm acesso.
    - Reportar qualquer incidente de segurança ou violação de dados imediatamente à equipe responsável.
    - Participar de treinamentos regulares sobre segurança da informação.
    - Utilizar somente os recursos autorizados pela organização para acessar, armazenar ou transmitir dados.

    2.2. Gerentes e Supervisores

    - Garantir que todos os colaboradores sob sua supervisão estejam cientes e cumpram as políticas de segurança da informação.
    - Promover uma cultura de segurança da informação por meio de treinamentos e conscientização regulares.
    - Supervisionar o acesso e o uso dos recursos de tecnologia da informação pelos colaboradores.
    - Notificar prontamente a equipe responsável sobre qualquer incidente de segurança ou violação de dados.

3. Uso Aceitável dos Recursos de TI

3.1. Acesso a Sistemas

- Os colaboradores devem utilizar suas credenciais individuais para acessar os sistemas autorizados.
- Não compartilhar senhas ou permitir o acesso não autorizado a sistemas ou informações confidenciais.

3.2. Uso de Dispositivos Móveis

- Seguir as políticas específicas de uso de dispositivos móveis estabelecidas pela organização.

- Proteger adequadamente os dispositivos móveis com senhas e recursos de segurança disponíveis.

3.3. Uso de E-mails e Comunicações Eletrônicas

- Utilizar o e-mail corporativo apenas para fins de trabalho e evitar o envio de informações confidenciais a destinatários não autorizados.
- Evitar abrir anexos ou clicar em links suspeitos ou provenientes de fontes desconhecidas.

4. Proteção de Dados

4.1. Classificação de Dados

- Conhecer e aplicar a política de classificação de dados da organização para determinar o nível adequado de proteção para cada tipo de informação.

4.2. Armazenamento e Transmissão de Dados

- Armazenar e transmitir os dados de forma segura, de acordo com as diretrizes estabelecidas pela organização.
- Utilizar sistemas e serviços aprovados para armazenar e compartilhar informações confidenciais.

5. Conscientização e Treinamento

- Participar de treinamentos regulares sobre segurança da informação oferecidos pela organização.
- Manter-se atualizado sobre as melhores práticas de segurança da informação e seguir as diretrizes fornecidas.

6. Cumprimento e Consequências

- O não cumprimento desta política pode resultar em ações disciplinares, incluindo advertências, suspensões ou rescisão de contrato, dependendo da gravidade da violação.

Esta política de segurança para os colaboradores visa garantir a proteção e confidencialidade das informações da nossa organização. Ao aderir a essas diretrizes, todos nós desempenhamos um papel essencial na preservação da segurança da informação.

Assinatura: _____

Nome: _____

Cargo: _____

Data: _____

POLÍTICA DE PRIVACIDADE

A política de privacidade é um documento fundamental para qualquer organização que coleta, armazena ou processa dados pessoais. Nele mostra aos titulares através dos canais de captação de dados a transparência com que seus dados serão tratados e a finalidade do mesmo. Este documento deve estar contido no site institucional para que os titulares tenham acesso de forma clara e fácil a estas informações.

EXEMPLO DE DOCUMENTO DE POLÍTICA DE PRIVACIDADE

Política de Privacidade

Esta Política de Privacidade descreve como coletamos, usamos e protegemos as informações pessoais que você fornece ao utilizar nossos serviços. Nós nos comprometemos a respeitar e proteger a sua privacidade e garantir a conformidade com as leis e regulamentações aplicáveis de proteção de dados.

1. Informações Coletadas Coletamos as seguintes informações pessoais quando você utiliza nossos serviços:

- Nome completo
- Endereço de e-mail
- Número de telefone
- Outras informações que você nos fornece voluntariamente

2. Uso das Informações Utilizamos as informações coletadas para:

- Fornecer os serviços solicitados por você
- Personalizar e melhorar a sua experiência com nossos serviços
- Enviar comunicações relevantes, como atualizações, notificações e ofertas especiais
- Realizar pesquisas e análises para melhorar nossos serviços
- Cumprir obrigações legais e regulatórias

3. Compartilhamento de Informações Não compartilhamos suas informações pessoais com terceiros, exceto nas seguintes circunstâncias:

- Quando necessário para fornecer os serviços solicitados por você
- Quando exigido por lei ou regulamento
- Com seu consentimento prévio

4. Segurança das Informações Adotamos medidas de segurança técnicas, administrativas e físicas adequadas para proteger suas informações pessoais contra acesso não autorizado, divulgação ou alteração. Implementamos controles

de acesso, criptografia de dados e proteção contra vírus e malware para garantir a segurança das informações.

5. Retenção de Informações Retemos suas informações pessoais pelo tempo necessário para cumprir as finalidades descritas nesta Política de Privacidade, a menos que um período de retenção mais longo seja exigido ou permitido por lei.
6. Seus Direitos de Privacidade Você tem o direito de acessar, corrigir, atualizar e excluir suas informações pessoais. Caso queira exercer esses direitos ou tenha dúvidas sobre nossas práticas de privacidade, entre em contato conosco por meio das informações de contato fornecidas no final deste documento.
7. Alterações na Política de Privacidade Reservamos o direito de atualizar ou modificar esta Política de Privacidade a qualquer momento, conforme necessário. Recomendamos que você reveja periodicamente esta política para se manter informado sobre nossas práticas de privacidade.
8. Contato Se você tiver dúvidas, comentários ou preocupações sobre nossa Política de Privacidade, entre em contato conosco através dos seguintes meios de contato:

Nome da Empresa: [Nome da Empresa]

Endereço: [Endereço da Empresa]

E-mail: [Endereço de E-mail]

Telefone: [Número de Telefone]

Data da última atualização: [Data da última atualização da Política de Privacidade]

Ao utilizar nossos serviços, você concorda com os termos desta Política de Privacidade e consente com a coleta, uso e armazenamento de suas informações pessoais conforme descrito neste documento.

TERMO DE CONSENTIMENTO

Este é um documento em que os titulares dos dados fornecem seu consentimento específico e informado para o tratamento de seus dados pessoais pela instituição.

Existem diferentes formas para obter o consentimento do titular dos dados, de acordo com a legislação de proteção de dados, como a LGPD. Alguns dos tipos de formas comuns para obtenção do consentimento são:

1. Consentimento por escrito: O titular dos dados assina um documento físico ou digital, manifestando seu consentimento de forma clara e específica.

2. Consentimento por meio eletrônico: O titular dos dados pode fornecer seu consentimento por meio de caixas de seleção, botões de confirmação ou cliques em "Aceitar" em formulários eletrônicos ou websites.

3. Consentimento verbal: O titular dos dados fornece seu consentimento oralmente, por exemplo, em uma ligação telefônica, gravação de voz ou em uma conversa presencial.

4. Consentimento implícito: Em determinadas situações previstas em lei, o consentimento pode ser considerado implícito, como quando o tratamento dos dados é necessário para a execução de um contrato ou para o cumprimento de uma obrigação legal.

5. Consentimento por meio de aplicativos ou sistemas: Em certos casos, o consentimento pode ser obtido por meio de aplicativos móveis, softwares ou sistemas específicos, em que o titular dos dados concorda com os termos e condições de uso.

Independentemente da forma utilizada, é importante garantir que o consentimento seja obtido de forma clara, específica, informada e inequívoca. Isso significa que o titular dos dados deve estar plenamente ciente das finalidades do tratamento, das informações a serem coletadas e compartilhadas, dos direitos que possui e da possibilidade de revogar o consentimento a qualquer momento.

Além disso, é fundamental que a instituição mantenha registros do consentimento obtido, incluindo informações sobre como e quando foi dado, para fins de comprovação da conformidade com a legislação de proteção de dados.

EXEMPLO DE DOCUMENTO DE CONSENTIMENTO

Termo de Consentimento para Tratamento de Dados Pessoais

Eu, [Nome completo do titular dos dados], CPF [Número do CPF], RG [Número do RG], residente no endereço [Endereço completo], declaro que li e compreendi as informações contidas neste termo e concordo em fornecer os meus dados pessoais à [Nome da Instituição], CNPJ [Número do CNPJ], para os fins descritos abaixo.

1. Finalidade do Tratamento: Autorizo o tratamento dos meus dados pessoais pela [Nome da Instituição] com a finalidade de [Descrever a finalidade específica, por exemplo: prestação de serviços, comunicação, oferta de produtos, cumprimento de obrigações legais, entre outros].

2. Dados Pessoais Coletados: Os dados pessoais que serão coletados e tratados incluem, mas não se limitam a:

- Nome completo
- Data de nascimento
- Endereço
- E-mail
- Número de telefone
- Informações profissionais
- Outros dados necessários para a finalidade específica.

3. Compartilhamento de Dados: Compreendo que a [Nome da Instituição] poderá compartilhar meus dados pessoais com terceiros, quando necessário para o cumprimento da finalidade descrita acima. Entendo que esses terceiros estão sujeitos a obrigações contratuais de confidencialidade e proteção dos dados.
4. Segurança dos Dados: Reconheço que a [Nome da Instituição] adota medidas técnicas e organizacionais adequadas para proteger os meus dados pessoais contra acesso não autorizado, perda, uso indevido ou divulgação.
5. Retenção dos Dados: Autorizo a [Nome da Instituição] a reter meus dados pessoais pelo tempo necessário para cumprir a finalidade descrita acima, respeitando os prazos estabelecidos pelas leis aplicáveis.
6. Direitos do Titular dos Dados: Estou ciente de que, como titular dos dados, tenho direito de acessar, retificar, atualizar e excluir meus dados pessoais, bem como de revogar o meu consentimento a qualquer momento, mediante solicitação à [Nome da Instituição].

Declaro ainda que sou maior de idade e que esta declaração é feita de forma livre e espontânea, sem qualquer tipo de coação ou influência externa.

Local e data: [Local e data em que o consentimento está sendo dado]

Assinatura: [Assinatura do titular dos dados]

Testemunha: Nome completo: [Nome completo da testemunha]

CPF: [Número do CPF da testemunha]

RG: [Número do RG da testemunha]

Registro das Atividades de Tratamento de Dados Pessoais: Documento que registra todas as atividades de tratamento de dados pessoais realizadas pela instituição, incluindo informações sobre os tipos de dados coletados, finalidades do tratamento, tempo de retenção, medidas de segurança adotadas, entre outros.

EXEMPLO DE REGISTRO DE ATIVIDADES DE TRATAMENTO DE DADOS PESSOAIS

Data de criação: [Data em que o registro foi criado]

Responsável pelo registro:

[Nome do responsável pelo registro]

Responsável pelo tratamento de dados:

[Nome da instituição ou departamento responsável pelo tratamento de dados]

1. Identificação do Tratamento:

    1.1. Nome do Tratamento: [Nome ou descrição do tratamento de dados]

    1.2. Finalidade do Tratamento: [Descreva de forma clara e específica a finalidade do tratamento de dados]

    1.3. Base Legal: [Indique a base legal que justifica o tratamento de dados, conforme previsto na legislação aplicável, como consentimento, execução de contrato, cumprimento de obrigação legal, interesse legítimo, entre outros]

    1.4. Categorias de Titulares dos Dados: [Descreva as categorias de indivíduos cujos dados pessoais serão tratados, por exemplo, clientes, funcionários, fornecedores]

    1.5. Categorias de Dados Pessoais: [Indique as categorias de dados pessoais que serão coletados e tratados, por exemplo, nome, endereço, e-mail, dados de pagamento]

    1.6. Categorias de Destinatários: [Descreva as categorias de destinatários com quem os dados pessoais podem ser compartilhados, como empresas parceiras, provedores de serviços, autoridades competentes]

2. Descrição das Operações de Tratamento:

    2.1. Coleta de Dados: [Explique como os dados pessoais são coletados, incluindo fontes de dados, métodos utilizados, formulários, sistemas, entre outros]

    2.2. Armazenamento: [Descreva como os dados pessoais são armazenados, como em servidores internos, nuvem, sistemas de terceiros, com medidas de segurança adotadas]

    2.3. Processamento: [Detalhe as atividades de processamento realizadas, como organização, estruturação, modificação, recuperação, consulta, exclusão dos dados]

2.4. Compartilhamento: [Indique com quem os dados pessoais podem ser compartilhados e com qual finalidade, incluindo terceiros, parceiros, fornecedores, autoridades]

2.5. Transferência Internacional de Dados: [Se aplicável, descreva se os dados pessoais serão transferidos para países fora do território nacional e quais medidas de segurança são adotadas para garantir a proteção dos dados transferidos]

3. Medidas de Segurança:

3.1. Medidas Técnicas: [Liste as medidas técnicas adotadas para proteger os dados pessoais, como criptografia, controle de acesso, monitoramento de rede]

3.2. Medidas Organizacionais: [Descreva as medidas organizacionais implementadas para garantir a segurança dos dados, como treinamentos, políticas internas, restrição de acesso]

3.3. Avaliação de Riscos: [Indique se foi realizada uma avaliação de riscos de segurança da informação e como os riscos foram identificados e gerenciados]

3.4. Incidentes de Segurança: [Informe como os incidentes de segurança são tratados, incluindo procedimentos de notificação, resposta e recuperação]

4. Retenção e Exclusão dos Dados:

4.1. Prazo de Retenção: [Especifique o prazo pelo qual os dados pessoais serão retidos, de acordo com a finalidade do tratamento e a legislação aplicável]

4.2. Exclusão dos Dados: [Descreva os procedimentos adotados para a exclusão segura dos dados pessoais após o término do prazo de retenção]

5. Registro de Consentimento:

5.1. Registro de Consentimento: [Caso o tratamento de dados seja baseado no consentimento, registre informações sobre como o consentimento é obtido e registrado]

Este Registro de Atividades de Tratamento de Dados Pessoais está em conformidade com a legislação aplicável, como a LGPD, e será mantido atualizado, refletindo todas as atividades de tratamento de dados realizadas pela instituição.

Relatório de Impacto à Proteção de Dados (DPIA):

Relatório de Impacto à Proteção de Dados (DPIA): Documento que descreve as avaliações de risco e impacto à proteção de dados realizadas pela instituição, especialmente em situações que envolvam tratamento de dados sensíveis ou de grande porte.

EXEMPLO DE RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS (DPIA):

Relatório de Impacto à Proteção de Dados (DPIA)

Data de elaboração: [Data em que o relatório foi elaborado]

Responsável pela elaboração: [Nome do responsável pela elaboração do relatório]
Responsável pelo tratamento de dados: [Nome da instituição ou departamento responsável pelo tratamento de dados]

1. Introdução:

O presente Relatório de Impacto à Proteção de Dados (DPIA) tem como objetivo analisar e avaliar os possíveis impactos à privacidade e proteção de dados decorrentes de um determinado projeto, processo ou atividade que envolve o tratamento de dados pessoais. A DPIA tem como base a legislação aplicável, como a LGPD, e visa identificar riscos, propor medidas mitigadoras e garantir a conformidade com os princípios e direitos dos titulares de dados.

2. Descrição do Projeto/Processo/Atividade:

2.1. Nome do Projeto/Processo/Atividade: [Nome ou descrição do projeto, processo ou atividade]

2.2. Finalidade do Tratamento: [Explique de forma clara e específica a finalidade do tratamento de dados]

2.3. Descrição do Tratamento: [Detalhe como os dados pessoais são coletados, armazenados, processados, compartilhados, transferidos, retidos e excluídos]

2.4. Categorias de Dados Pessoais: [Indique as categorias de dados pessoais que são tratadas no projeto, processo ou atividade]

2.5. Base Legal: [Identifique a base legal que justifica o tratamento de dados, conforme previsto na legislação aplicável]

3. Análise de Riscos:

3.1. Identificação dos Riscos: [Enumerar os riscos potenciais à privacidade e proteção de dados decorrentes do tratamento]

3.2. Avaliação dos Riscos: [Analisar a probabilidade de ocorrência e o impacto dos riscos identificados]

3.3. Medidas Mitigadoras: [Propor medidas para mitigar os riscos identificados, como implementação de controles de segurança, revisão de processos, treinamento de colaboradores]

3.4. Análise de Alternativas: [Analisar possíveis alternativas para o tratamento de dados que possam reduzir os riscos identificados]

3.5. Consulta a Stakeholders: [Descrever a consulta realizada a stakeholders relevantes, como titulares de dados, especialistas em proteção de dados, representantes da empresa]

4. Conclusões e Recomendações:

4.1. Conclusões: [Apresentar as conclusões da análise de riscos e avaliação dos impactos à privacidade e proteção de dados]

4.2. Recomendações: [Propor recomendações para mitigar os riscos e garantir a conformidade com a legislação de proteção de dados]

5. Responsabilidades e Cronograma:

5.1. Responsabilidades: [Indicar as responsabilidades dos envolvidos na implementação das medidas mitigadoras]

5.2. Cronograma: [Definir um cronograma para a implementação das recomendações e monitoramento das ações realizadas]

Este Relatório de Impacto à Proteção de Dados (DPIA) foi elaborado de acordo com a legislação aplicável e serve como documento de referência para a análise e avaliação dos impactos à privacidade e proteção de dados em projetos, processos ou atividades que envolvam o tratamento de dados pessoais.

PARA UM ENTENDIMENTO MELHOR VAMOS COLOCAR O DOCUMENTO ACIMA COM DADOS FICTICIOS

Relatório de Impacto à Proteção de Dados (DPIA)

Data de elaboração: 15 de julho de 2023 Responsável pela elaboração: João Silva Responsável pelo tratamento de dados: Instituição Beneficente ABC

1. Introdução:

O presente Relatório de Impacto à Proteção de Dados (DPIA) tem como objetivo analisar e avaliar os possíveis impactos à privacidade e proteção de dados decorrentes do projeto "Programa de Doações Online". A DPIA tem como base a legislação aplicável, como a Lei Geral de Proteção de Dados (LGPD), e visa identificar riscos, propor medidas mitigadoras e garantir a conformidade com os princípios e direitos dos titulares de dados.

2. Descrição do Projeto:

2.1. Nome do Projeto: Programa de Doações Online 2.2. Finalidade do Tratamento: Coletar e processar dados pessoais de doadores para realizar doações online em benefício de causas sociais. 2.3. Descrição do Tratamento: Os dados pessoais dos doadores são coletados por meio de um formulário online que inclui informações como nome, endereço de e-mail, telefone e valor da doação. Esses dados são armazenados em um sistema seguro e utilizados para processar as doações, emitir recibos e manter contato com os doadores. 2.4. Categorias de Dados Pessoais: Nome, endereço de e-mail, telefone. 2.5. Base Legal: Consentimento do titular dos dados para o tratamento das informações conforme previsto na LGPD.

3. Análise de Riscos:

3.1. Identificação dos Riscos:

- Risco de acesso não autorizado aos dados pessoais dos doadores
- Risco de perda ou vazamento dos dados pessoais durante o armazenamento ou transmissão
- Risco de uso indevido dos dados pessoais para fins não autorizados

3.2. Avaliação dos Riscos:

- Probabilidade: Moderada
- Impacto: Significativo

3.3. Medidas Mitigadoras:

- Implementação de medidas de segurança, como criptografia e controle de acesso, para proteger os dados pessoais contra acesso não autorizado
- Utilização de servidores e sistemas confiáveis para o armazenamento dos dados pessoais
- Políticas e procedimentos claros para o uso dos dados pessoais somente para os fins autorizados

3.4. Análise de Alternativas:

- Avaliação de provedores de serviços de doações online que possuam certificações de segurança reconhecidas
- Verificação de alternativas para minimizar a coleta de dados pessoais sensíveis, solicitando apenas informações essenciais para a realização das doações

3.5. Consulta a Stakeholders:

- Consulta aos doadores por meio de questionários online para avaliar a percepção de segurança e privacidade no programa de doações online
- Diálogo com especialistas em proteção de dados para obter recomendações adicionais

4. Conclusões e Recomendações:

4.1. Conclusões:

- Os riscos identificados podem afetar a privacidade e a proteção dos dados pessoais dos doadores no programa de doações online.
- As medidas mitigadoras propostas, como a implementação de medidas de segurança e a seleção de provedores confiáveis, são essenciais para reduzir os riscos identificados.

4.2. Recomendações:

- Implementar medidas de segurança, como criptografia e autenticação de usuários, para proteger os dados pessoais dos doadores.
- Realizar auditorias periódicas nos sistemas e procedimentos para garantir a conformidade com a LGPD.
- Manter um registro das atividades de tratamento de dados pessoais realizadas no âmbito do programa de doações online.

5. Responsabilidades e Cronograma:

5.1. Responsabilidades:

- Equipe de TI: Implementação das medidas de segurança e monitoramento dos sistemas.
- Equipe de Recursos Humanos: Treinamento dos colaboradores sobre a LGPD e a importância da proteção de dados pessoais.
- Equipe de Gestão: Supervisão do cumprimento das medidas mitigadoras e do registro das atividades de tratamento de dados.

5.2. Cronograma:

- Implementação das medidas de segurança: Até 31 de agosto de 2023
- Treinamento dos colaboradores: Setembro de 2023
- Auditorias periódicas: A cada 6 meses

Este Relatório de Impacto à Proteção de Dados (DPIA) foi elaborado com o intuito de garantir a conformidade com a LGPD e proteger a privacidade e a segurança dos dados pessoais dos doadores no âmbito do programa de doações online da Instituição Beneficente ABC.

POLÍTICA DE RETENÇÃO DE DADOS

Política de Retenção de Dados: Documento que define os períodos de retenção dos dados pessoais, ou seja, por quanto tempo a instituição irá armazenar os dados antes de excluí-los de forma segura.

O Ideal é colocar os dados em uma planilha e identificar a retenção de cada um dos dados conforme sua finalidade.

EXEMPLO DE PLANILHA DE POLÍTICA DE RETENÇÃO DE DADOS

Tipo de Dado	Finalidade	Base Legal	Prazo de Retenção	Responsável
Dados dos Colaboradores	Gestão de Recursos Humanos	Legislação Trabalhista	Durante o vínculo empregatício + prazo adicional exigido pela legislação	Departamento de RH
Dados dos Doadores	Manter relacionamento e enviar comunicações	Consentimento do Doador	Enquanto houver interesse do doador em receber comunicações	Departamento de Captação de Recursos
Dados dos Beneficiários	Execução de programas assistenciais	Execução de contrato ou consentimento do beneficiário	Prazo necessário para cumprir as finalidades + prazo adicional exigido pela legislação	Departamento de Assistência Social
Outros Dados Pessoais	[Descreva outros tipos de dados pessoais coletados]	[Base legal específica]	[Prazo específico de retenção]	[Departamento responsável]

Nessa planilha, você pode listar os diferentes tipos de dados pessoais coletados pela instituição, suas finalidades, a base legal para o tratamento, o prazo de retenção e o departamento responsável por esses dados. Essa planilha ajudará a documentar e manter um registro claro das políticas de retenção de dados da instituição.

EXEMPLO DE DOCUMENTO DE RETENÇÃO DE DADOS

Política de Retenção de Dados

Data de vigência: 1º de janeiro de 2024

1. Introdução

A Política de Retenção de Dados estabelece as diretrizes e procedimentos para a retenção e o descarte adequados dos dados pessoais coletados e processados pela Instituição Beneficente XYZ. Esta política é baseada na legislação aplicável, incluindo a

Lei Geral de Proteção de Dados (LGPD), e tem como objetivo garantir a conformidade com as obrigações legais e proteger a privacidade dos titulares de dados.

2. Princípios de Retenção de Dados

2.1. Minimização de Dados: A Instituição Beneficente XYZ se compromete a coletar e reter apenas os dados pessoais estritamente necessários para cumprir as finalidades específicas do tratamento.

2.2. Prazo de Retenção: Os dados pessoais serão retidos pelo período necessário para cumprir as finalidades do tratamento, conforme estabelecido na legislação aplicável e nas políticas internas da instituição.

2.3. Revisão e Atualização: Os prazos de retenção serão revisados periodicamente para garantir que os dados pessoais sejam mantidos apenas pelo tempo necessário.

2.4. Descarte Seguro: Após o término do prazo de retenção, os dados pessoais serão descartados de forma segura, garantindo que não haja acesso não autorizado ou uso indevido das informações.

3. Responsabilidades

3.1. Diretoria: É responsável por definir e aprovar os prazos de retenção de dados pessoais com base nas finalidades do tratamento e na legislação aplicável.

3.2. Gestores de Departamento: São responsáveis por garantir a aplicação correta da política de retenção de dados em suas respectivas áreas.

3.3. Equipe de TI: É responsável por implementar as medidas técnicas necessárias para garantir o descarte seguro dos dados pessoais, incluindo a destruição física ou a exclusão definitiva dos registros.

4. Prazos de Retenção de Dados

4.1. Dados dos Colaboradores: Os dados pessoais dos colaboradores serão retidos pelo período em que o vínculo empregatício estiver ativo e pelo prazo adicional exigido pela legislação trabalhista e previdenciária.

4.2. Dados dos Doadores: Os dados pessoais dos doadores serão retidos pelo período necessário para cumprir as finalidades da doação e para manter o relacionamento com os doadores. Após o término desse período, os dados serão anonimizados ou descartados de forma segura.

4.3. Dados dos Beneficiários: Os dados pessoais dos beneficiários serão retidos pelo período necessário para cumprir as finalidades do programa assistencial e para atender aos requisitos legais.

4.4. Outros Dados Pessoais: Para outros tipos de dados pessoais coletados e processados pela instituição, serão estabelecidos prazos de retenção específicos, levando em consideração as finalidades do tratamento e as obrigações legais.

5. Descarte de Dados

5.1. Descarte Físico: Os documentos físicos que contenham dados pessoais serão destruídos de forma segura por meio de trituração, incineração ou outro método adequado, garantindo a impossibilidade de recuperação das informações.

5.2. Descarte Eletrônico: Os dados pessoais armazenados em meio eletrônico serão excluídos de forma definitiva e segura dos sistemas, utilizando métodos que impeçam a sua recuperação.

6. Revisão da Política

Esta Política de Retenção de Dados será revisada periodicamente para garantir sua eficácia e conformidade com a legislação aplicável. Alterações serão feitas conforme necessário e comunicadas a todos os colaboradores da Instituição Beneficente XYZ.

Assinaturas:

Presidente ou dirigente da Instituição

Data: _____

DOCUMENTOS FINAIS QUE DEVEM SER CRIADOS E MANTIDOS PELA INSTITUIÇÃO

Com a implementação e vigência da LGPD, as instituições devem produzir e manter atualizados os seguintes documentos abaixo que foram bem detalhados no decorrer deste e-book. Estes Dcoumentos servem como base para uma possível auditoria verificarem que as insitutições estão seguindo a lei.Os documentos são:

Política de Privacidade

Termo de Consetimento

Registro de Atividades e Tratamento de Dados Pessoais

Relatório de Impacto a Proteção de DAdos (DPIA)

Contratos com Terceiros

Política de Segurança da Informação

Política de Retenção de Dados

CONCLUSÃO

A Lei Geral de Proteção de Dados (LGPD) trouxe mudanças significativas para as instituições beneficentes, exigindo uma série de medidas para garantir a proteção dos dados pessoais dos indivíduos. Neste contexto, a conscientização, o treinamento e a implementação de políticas e procedimentos adequados são fundamentais.

Para se adequar à LGPD, as instituições beneficentes devem mapear os dados pessoais que possuem, documentar os fluxos de dados, analisar os riscos envolvidos, implementar medidas de segurança da informação, estabelecer contratos com terceiros contendo cláusulas de LGPD e desenvolver processos eficientes para responder a incidentes de segurança.

A conscientização e o treinamento dos colaboradores também são essenciais. É importante promover uma cultura de proteção de dados, fornecer informações sobre a LGPD, seus princípios e impactos, e orientar os colaboradores sobre suas responsabilidades no tratamento adequado dos dados pessoais.

Além disso, a documentação desempenha um papel crucial na conformidade com a LGPD. A criação de documentos como políticas de segurança da informação, política de privacidade, inventário de dados pessoais, registro de atividades de tratamento de dados e políticas de retenção de dados é fundamental para garantir a transparência e a conformidade com a legislação.

Em resumo, a adequação à LGPD requer um esforço contínuo por parte das instituições beneficentes. Ao adotar uma abordagem abrangente, que envolva conscientização, treinamento e implementação de políticas e procedimentos adequados, as instituições podem proteger os dados pessoais dos indivíduos, fortalecer a confiança e manter a conformidade com a lei.

AGRADECIMENTO

Agradecemos a você, caro leitor, por dedicar seu tempo para ler este e-book. Esperamos que as informações fornecidas tenham sido úteis e tenham ajudado a esclarecer suas dúvidas sobre a LGPD e sua aplicação nas instituições beneficentes.

Nosso objetivo é fornecer orientações claras e úteis para auxiliá-lo no processo de conformidade com a LGPD. Se você tiver mais perguntas ou precisar de informações adicionais, não hesite em entrar em contato.

A proteção dos dados pessoais é uma responsabilidade compartilhada, e sua disposição em aprender e implementar as melhores práticas é fundamental. Ao adotar as medidas necessárias para proteger os dados pessoais das pessoas envolvidas em sua instituição beneficente, você está contribuindo para a segurança e a privacidade de todos.

Agradecemos novamente por sua leitura e por fazer parte desse importante movimento em direção à proteção dos dados pessoais. Desejamos sucesso em sua jornada de conformidade com a LGPD e estamos aqui para apoiá-lo sempre que necessário.

Atenciosamente,

SINIBREF

REFERENCIAS

"LGPD: Registro das operações de tratamento de Dados Pessoais"

Autor: Cláudio Dodt

URL: https://www.udemy.com/

"LGPD: Relatório de Impacto à Proteção de Dados Pessoais"

Autor: Cláudio Dodt

URL: https://www.udemy.com/

"LGPD: Legítimo interesse - teoria e prática!"

Autor: Cláudio Dodt

URL: https://www.udemy.com/

"Lei geral de Proteção de Dados Pessoais na Prática"

Autor: Daniel Donda

URL: https://www.udemy.com/

Curso Instituto Euvaldo Lodi - Lei Geral de Proteção de Dados Pessoais Teoria e Prática

Autor:João Araújo Monteiro Neto - Ano de Publicação: 2021

OpenAi - CHAT GPT

Lei nº13.709/2018

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm