FUNDACRED

Um *framework*[1] *multistakeholder* para conscientização sobre os princípios gerais da

Lei Geral de Proteção de Dados

(LGPD)

Fundacred, novembro de 2019
Por **Nivio Júnior Lewis Delgado** | Diretor Executivo

[1] Um *framework* provê soluções, incorporadas em um design abstrato, para uma família de problemas inter-relacionados.

Sumário

Sumário

1 O Porquê da Fundacred Estar Promovendo a Conscientização de Seus *Stakeholders*

Nossa Reputação É Nosso Cartão de Visita.

Em uma sociedade descentralizada, em que a agilidade pauta nossas estratégias, projetos e iniciativas, ao mesmo tempo que somos avaliados, constantemente, quanto à qualidade integral de nossa entrega, alocar recursos para distribuir soluções que não estejam diretamente atreladas ao *core* da sua oferta, mas que proporcionem percepção de valor por parte de seus *stakeholders*, é demonstração de lealdade e inteligência.

A Fundacred tem em seu DNA o pioneirismo desde sua fundação. Foi a primeira organização a trazer o conceito e implantar o crédito educacional no Brasil, em 1972. Também foi uma das primeiras companhias a digitalizar documentos no Brasil, ainda na década de 1990, e a utilizar sistemas operacionais *open source* no início dos anos 2000. Atualmente, autodefine-se como uma organização do terceiro setor, sem fins lucrativos, muito tradicional e consistente, mas com espírito de *startup*.

Desde 2017, temos um Comitê de Segurança da Informação ligado diretamente à direção e, a partir de 2018, implantamos um programa específico para recepcionar

a Lei Geral de Proteção de Dados, dispositivo legal que dispõe sobre normas internacionalmente consagradas, gerando convergência e dando melhor sentido para alguns princípios e regras já previstos no ordenamento jurídico brasileiro.

Em 2019, nosso time de gerentes, supervisores e coordenadores recebeu treinamentos, ultrapassando centenas de horas em capacitações. Todas as áreas da organização participaram e ainda participam dessa jornada. Provedores de conteúdo e especialistas em Direito Digital, Privacidade e Proteção de Dados como Insper, Opice Blum Academy e Data Privacy Academy foram fundamentais para nossa conscientização.

Desde a concepção do programa, tínhamos consciência de que esta seria uma oportunidade valiosa de, novamente, colaborarmos com a construção de um ambiente de melhor convivência onde atuamos. De imediato, houve uma forte identificação do time com os princípios que a LGPD trouxe.

No decorrer do processo de implantação do programa e durante a jornada de implementação, percebemos o quanto de ganho, tangível e intangível, poderíamos obter. Inúmeros processos que já considerávamos *lean* foram revistos e tornados ainda mais enxutos, gerando economias importantes, além da redução de resíduos, inclusive digitais.

Tudo isso é importante, sem dúvida, mas o que mais nos encanta (apaixona) nessa jornada é a possibilidade de gravar em nossos processos e na nossa oferta valores já presentes em nossa organização, como **Valorização das Pessoas**, **Integridade**, **Sucesso do Cliente**, **Desenvolvimento Sustentável** e, é claro, **Transformação**.

Sabemos que ter excelência operacional em escala, sendo a melhor em recuperação de ativos de crédito educacional no Brasil, não nos coloca em situação de conforto. Temos consciência de que ser a melhor opção no Brasil, para instituições de ensino e para estudantes, no quesito “menor custo privado”, igualmente, não é suficiente. O fato de termos esses diferenciais competitivos, ou “pontos de diferença”, não impede que sejamos copiados e/ou substituídos. Por outro lado, temos presente que, ao estabelecer um ponto de vista a ser perseguido para nos manter como a melhor, não “do mercado, mas para o mercado”, nos coloca em evidência

constante, o que só fortalece nosso desejo de colaboração.
Esperamos que você faça o melhor uso possível dessa ferramenta, para garantir às pessoas a possibilidade de exercer o seu direito humano e fundamental à privacidade.

Nivio Júnior Lewis Delgado
Diretor Executivo da Fundacred
@niviodelgado
br.linkedin.com › niviodelgado

"Nosso talento, nosso propósito:
Transformar vidas, promovendo acesso à educação."

2 Utilidade e Usabilidade

Na sociedade da informação, em que o fluxo informacional é onipresente, é cada vez mais difícil garantir a privacidade e a proteção adequada de dados pessoais. Implantar e manter a governança nas organizações é um meio eficaz de mitigação de riscos nas decisões dos negócios e nas operações do dia a dia.

Optamos por evidenciar os princípios gerais por entendermos que são as verdades fundamentais que a LGPD nos traz. Assim como os três princípios consolidados da Segurança da Informação (**Integridade**, **Disponibilidade** e **Confidencialidade**) pautaram - e ainda pautam - nossas relações com nossos *stakeholders*, os princípios de Privacidade e Proteção de Dados têm proporcionado a convergência de verdades globais para a criação, atualização, interpretação e aplicação das normas positivadas em países ocupados com o tema.

Temos consciência de que a natural evolução da sociedade estabelece uma corrida em que a tecnologia e os mercados são a veloz lebre e o Estado e seu ordenamento é, por vezes, a tartaruga. Portanto, ter princípios basilares e verdadeiros são fundamentais para equilibrarmos a vida ágil dos dias de hoje aos desejos do Estado (e por conseguinte da sociedade), transcritos em normas muitas vezes consolidadas de forma vagarosa e, por vezes, caduca.

O Brasil acertou ao escolher promulgar uma lei de forte caráter principiológico e, a Fundacred, inspirada em modelos internacionais, desenvolveu esta ferramenta

de conscientização e autoavaliação, igualmente orientada pelos princípios da LGPD, para colaborar com seus *stakeholders* na concepção, desenvolvimento e implementação de uma boa governança de dados pessoais. A autoavaliação utilizando esse *framework* é um processo pelo qual uma organização inicia uma reflexão, com a finalidade de *benchmarking*, para melhorar seus processos e práticas de privacidade ao longo do tempo. Temos a pretensão de levar aos nossos *stakeholders*, para que possam verificar seus níveis de conformidade, um conjunto de expectativas principiológicas presentes na LGPD. **Desejamos que, com a autoavaliação, as organizações possam identificar lacunas e/ou riscos presentes em seus processos e nas suas ofertas, endereçando soluções mais conscientes.**

Esta ferramenta é oferecida como sugestão gratuita para guiar organizações na avaliação e melhoramento de seus processos, produtos ou serviços que fazem algum tipo de tratamento de dados pessoais. O *framework* é projetado para organizações que estão sujeitas à Lei Geral de Proteção de Dados (LGPD) e não tem a pretensão de esgotar o *assessment* ao qual todas as destinatárias da lei necessitam se submeter para endereçar boas práticas e a conformidade com a legislação vigente, tendo em vista um conjunto de outros dispositivos legais existentes no ordenamento jurídico brasileiro, tais como Marco Civil da Internet (MCI), Regulamento do MCI, Código de Defesa do Consumidor, Estatuto da Criança e do Adolescente, Regulamentos e Normativas de setores específicos.

O uso dessa ferramenta é voluntário. Como você irá implantar, implementar ou mesmo obter sucesso ao alcançar a conformidade com a LGPD é de sua responsabilidade. Nada neste documento de consulta deve ser considerado para interferir ou vincular a Fundacred às suas responsabilidades, especialmente com relação a qualquer reclamação apresentada por um titular, cujos dados pessoais estejam sob sua responsabilidade ou em relação à Autoridade Nacional de Proteção de Dados e demais órgãos de proteção de direitos dos respectivos titulares.

O que É Essa Ferramenta?

- Um conjunto de diretrizes que organizações podem utilizar para monitorar o cumprimento dos 10 princípios da LGPD;

- Um quadro de princípios e critérios para avaliar o nível de aderência da sua organização aos princípios da LGPD;

- E um meio de interpretação dos resultados da autoavaliação que permite criar um plano de ação para melhorar suas práticas de governança de dados pessoais, comparando-as com práticas de governança internacionais já em vigor.

O que Essa Ferramenta Não É?

- Uma “bala de prata” para a conformidade a ser aplicada por sua organização;

- Um substituto para métodos de avaliação recomendados por assessorias e consultorias especializadas que você pode já ter implementado;

- Definitiva e abrangente para todas as organizações;

- Ou a reposição ou substituição para a LGPD e demais normas do ordenamento jurídico.

Como Usar Essa Ferramenta

A ferramenta é composta de duas partes, sendo que ambas são descritas em mais detalhes nas seções posteriores:

Parte 1

O Guia de Avaliação para uma Governança de Dados Pessoais ajudará a informá-lo de suas obrigações em relação aos princípios da LGPD;

Parte 2

O *Checklist* de Autoavaliação é uma série de listas de verificação que você pode usar para avaliar o quão compatível estão sua oferta, seus processos e procedimentos em relação aos princípios da LGPD.

Esta ferramenta pode ser adaptada para aplicação em sua organização como um

todo ou a determinadas áreas e/ou unidades de negócios. Se você não tem um programa de privacidade e proteção de dados estabelecido, ou um Programa de Governança de Dados Pessoais, como denominamos na Fundacred, poderá usá-la para identificar os vários controles de privacidade (políticas, sistemas, procedimentos, controles de acesso, etc.) que precisam ser concebidos, implantados e implementados dentro de sua organização. Após implantação e implementação dos controles, use as listas de verificação para realizar uma autoavaliação minuciosa periodicamente, para identificar as lacunas e pontos de melhoria nas práticas de governança de dados pessoais. Atualize essa ferramenta conforme a evolução legislativa e de acordo com a realidade da sua organização. O importante é iniciar e manter atualizada a reflexão sobre Privacidade e Proteção de Dados em sua organização.

Apêndice A: FAQ - Perguntas frequentes.
Apêndice B: Bibliografia e fontes confiáveis de consulta.

3 Parte 1: Guia de Avaliação Para Uma Governança de Dados com Base nos Princípios da LGPD

Introdução

Este Guia de Avaliação para uma Governança de Dados vai ajudá-lo a desenvolver boas práticas de privacidade e proteção de dados sob uma perspectiva dos princípios da LGPD, ou seja, não pode ser considerado como único instrumento para a avaliação de sua conformidade em relação à Proteção de Dados e Privacidade.

Cada seção deste guia descreve um dos 10 princípios da Lei Geral de Proteção de Dados e, portanto, uma das bases normativas para uma Governança de Dados Pessoais, permitindo uma autoavaliação parcial em relação à conformidade com a LGPD.

A fim de avaliar a conformidade de sua organização em relação às políticas e práticas compatíveis com os princípios da LGPD, você deve abordar os critérios associados a cada princípio. O guia descreve atividades e melhores práticas para atingir os objetivos de cada um dos 10 princípios da LGPD.

Atenção: Este *framework* é exemplificativo e genérico, pode ser necessário adaptá-lo ou escolher formas específicas de implantar e implementar práticas que atendam os requisitos da legislação em vigor.

Os princípios da LGPD (Boa-fé + 10):

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 (LGPD)

Art. 6º - As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Princípio I - Da Finalidade

Art. 6º, Inciso I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Como atingir os objetivos desse princípio?

Você deve fazer um esforço razoável para garantir que o titular dos dados tenha sido informado das finalidades para as quais serão tratados seus dados, de uma maneira tal que o titular possa entender como seus dados serão utilizados.

- Identifique e documente seus propósitos legítimos para o tratamento de dados pessoais;
- Informe aos titulares, explicitamente, a finalidade para a qual está tratando seus dados pessoais;
- Determine as quantidades e os tipos de dados pessoais necessários para cumprir com a finalidade identificada, em atenção aos princípios da "Adequação" e da "Necessidade", proporcionando coerência no tratamento de dados pessoais;
- Reveja suas práticas atuais e determine os fins específicos para a coleta e demais casos de tratamento de dados pessoais;
- Revise os propósitos da sua atividade de tratamento de dados pessoais, mesmo que legítimos, para determinar se são apropriados, considerando a mitigação de quaisquer riscos de privacidade potenciais decorrentes;
- Confirme se as razões pelas quais você está tratando dados pessoais são o que uma pessoa razoável (um cliente típico) poderia esperar ou considerar apropriado em circunstâncias normais da relação negocial;
- Identifique de forma clara as atividades de coleta - e demais tratamentos de dados pessoais - que são essenciais e aqueles que não são, para o real fornecimento dos produtos e/ou serviços. Os titulares de dados pessoais devem

ser capazes de optar por não concordar com o tratamento de dados para fins não essenciais ou secundários da prestação de serviços ou fornecimento de produtos de sua organização;

- Mantenha registro de todas as razões pelas quais você coleta e realiza outra modalidade de tratamento de dados pessoais. Mantenha essa documentação atualizada;

- Seja específico sobre as finalidades divulgadas para o tratamento de dados pessoais;

- Não use grandes categorias de finalidades, tais como “servir ao cliente”;

- Evite linguagem vaga ou dúbia como “... e outros usos apropriados”;

- Use termos claros, concretos e inequívocos, para que os clientes (titulares) sejam capazes de compreender as finalidades para as quais a sua organização pretende tratar dados pessoais;

- Para respeitar o “Princípio da Transparência”, incorpore as declarações de propósito em suas políticas de privacidade e em outros documentos relevantes (por exemplo, contratos, regulamentos e formulários);

- Especifique as finalidades para as quais está tratando dados;

- Empenhe-se para informar aos seus clientes a respeito dos propósitos para os quais a sua organização pretende tratar dados pessoais.

Ao especificar **oralmente** as finalidades para as quais está tratando dados:

- Treine o time que coleta dados pessoais de modo que eles sejam capazes de informar com precisão, de forma clara e consistente, as finalidades para as quais estão coletando dados, bem como para informar os titulares de quaisquer novas razões para a coleta;

- Forneça um *script* padrão ou use outros meios para garantir que todos do time possam informar tais fins para os clientes (titulares de dados pessoais) de forma clara e consistente;

- Se a sua organização registra chamadas telefônicas com os titulares de dados (por exemplo, para fins de controle de qualidade), estabeleça uma prática de informar ao titular sobre essa conduta e seus efeitos, no início de cada chamada.

Ao especificar **por escrito** as finalidades para as quais está tratando dados:

- Forneça ao titular declarações a respeito das finalidades para as quais está tratando seus dados, antes ou de preferência no momento da coleta dos dados pessoais do titular;

- Em quaisquer materiais escritos, usados para notificar os clientes (titulares de dados), certifique-se de que as declarações de finalidade estão em locais fáceis de encontrar, ler e entender. Use uma linguagem simples sempre que possível.

Princípio II - Da Adequação

Art. 6º, Inciso II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

Como atingir os objetivos desse princípio?

Você só pode tratar dados pessoais para uma nova finalidade se isso for compatível com a finalidade original, se obtiver consentimento ou se tiver uma permissão legal específica.

- Identifique claramente a finalidade para a qual está tratando dados pessoais;

- Colete dados pessoais apenas por meios legítimos, obedecendo o princípio da boa-fé (sem induzir a erro ou enganar o titular) sobre os propósitos legítimos para a coleta e demais tratamentos;

- Especifique quais tipos de dados pessoais estão sendo coletados e/ou tratados como parte das políticas de tratamento de dados pessoais da organização, em atenção ao "Princípio da Transparência";

- Se pretende utilizar dados pessoais para uma nova finalidade, verifique se é compatível com a finalidade e propósitos legítimos originais, de acordo com o contexto do tratamento, ou obtenha o consentimento específico para o novo propósito/finalidade;

- Documente a finalidade para a qual está tratando os dados pessoais;

- Inclua detalhes dos seus legítimos propósitos em seus avisos e políticas de privacidade;

- Trate dados pessoais observando se os procedimentos realizados são compatíveis com as finalidades informadas ao titular dos dados pessoais;

- Analise regularmente seus processos internos e, quando necessário, atualize-os e sua respectiva documentação, bem como a política de privacidade;

- Determine prazos de temporalidade para tratamento de dados pessoais para que não sejam tratados por prazo superior àquele suportado pela finalidade e pela base legal de tratamento.

Princípio III - Da Necessidade

Art. 6º, Inciso III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Como atingir os objetivos desse princípio?

Você deve garantir que os dados pessoais que está tratando sejam limitados ao necessário, ou seja, que não possui mais do que precisa para a finalidade declarada aos titulares, além daqueles suficientes para cumprir adequadamente o objetivo declarado e que possuam um vínculo relacional com esse objetivo.

- Limite a coleta e demais procedimentos de tratamento de dados pessoais (quantitativamente e qualitativamente) ao que é necessário para a finalidade declarada ao titular;

- Verifique se sua organização coleta dados pessoais de forma consistente e legítima e se não coleta de forma indiscriminada ou com equívocos quanto às finalidades;

- Determine por que sua organização coleta dados pessoais, e quais as quantidades mínimas e tipos de dados necessários para cumprir essas finalidades;

- Faça uma distinção clara entre os dados obrigatórios e os opcionais. Alguns dados-chave são necessários para fornecer um produto ou serviço, enquanto outros podem ser úteis, mas não necessários. Designar o que é "desejável" como opcional para o consumidor é uma medida de lealdade e boa-fé;

- Limite a coleta de dados pessoais da sua organização para quantidades mínimas e tipos (qualidades) necessários para as finalidades identificadas e declaradas. Os dados não devem ser coletados e tratados com base em sua "utilidade no futuro";

- Sempre que possível, faça uso de anonimização de dados, o que os torna "não pessoais" ou, ainda, pseudonimização de dados para, por exemplo, identificar um cliente por um número em vez de um nome;

- Comunique-se de forma a atender o "Princípio da Transparência", especificando claramente os tipos (qualidades) e quantidades de dados coletados, bem como as finalidades para a coleta;

- Atribua fins específicos para tipos específicos de dados pessoais;

- Certifique-se da origem e legitimidade dos dados pessoais coletados a partir de qualquer fonte, mesmo as que não venham dos próprios clientes titulares dos dados pessoais (por exemplo, *marketplaces*, birôs de crédito, empresas de cobrança, marketing digital);

- Estabeleça procedimentos para coleta de dados pessoais e certifique-se de que todos compreendem e respeitam os limites da coleta;

- Ao notificar os clientes, oralmente ou por escrito, por que você está coletando informações, faça clara distinção entre o que é obrigatório e o que é opcional. Informações opcionais são apenas úteis, diferentemente das necessárias.

Princípio IV - Do Livre Acesso

Art. 6º, Inciso IV - livre acesso: garantia aos titulares de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

Como atingir os objetivos desse princípio?

Você deve garantir aos titulares o livre acesso, por meio de consulta gratuita, de seus dados pessoais, da existência ou não de tratamento desses dados, duração e integridade das informações constantes a seu respeito.

- Ao receber um pedido do titular ou por representante legalmente constituído, você deverá observar os prazos e os termos previstos em regulamento, que será expedido pela Autoridade Nacional de Proteção de Dados (ANPD), sem qualquer custo ao titular:
  - informar os titulares dos dados pessoais se está ou não tratando seus dados;
  - permitir o acesso individual aos dados tratados;
  - fornecer:
    - as finalidades para as quais usa seus dados;
    - forma e duração do tratamento, observando os segredos comercial e industrial;
    - identificação do controlador (especialmente quando estiver tratando na

condição de operador);
- informações de contato do controlador;
- informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
- responsabilidades dos agentes que realizarão o tratamento;
- uma relação com os direitos do titular, com menção explícita aos direitos contidos no art. 18 da LGPD:
    - confirmação da existência de tratamento;
    - acesso aos dados;
    - correção de dados incompletos, inexatos ou desatualizados;
    - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta lei;
    - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
    - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta lei;
    - informações das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
    - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
    - revogação do consentimento, nos termos da LGPD;
    - peticionar em relação aos seus dados contra o controlador perante a autoridade nacional;
    - opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta lei.

- Envie ao titular, em caso de impossibilidade de adoção imediata das previdências de que trata a LGPD, no tocante à revogação de consentimento, suspensão, eliminação de dados, portabilidade, anonimização, bloqueio e demais medidas, resposta em que poderá:
    - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente;
    - ou indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

- Informe, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional;

- Seja o mais específico possível sobre terceiros aos quais sua organização tenha transmitido dados pessoais e quais dados foram transmitidos;

- Garanta que sua política de privacidade inclua procedimentos para o tratamento dos pedidos de livre acesso aos dados pessoais por parte de seus titulares;

- Certifique-se de que seus sistemas de informação podem localizar os dados pessoais dos titulares requisitantes, incluindo os transmitidos a terceiros, e que os dados solicitados podem ser obtidos com o mínimo de interrupção das operações;

- Assegure-se de que o time designado para processar pedidos de acesso tem consciência de suas responsabilidades em relação ao "Princípio do Livre Acesso", bem como os procedimentos específicos e prazos a serem observados, como também as exceções aplicáveis, especialmente quanto à suspensão e bloqueio de tratamento, eliminação, atualização e/ou correção de dados pessoais;

- Assegure-se de que o time sabe como identificar um pedido de acesso e submetê-lo ao encarregado de dados ou ao comitê apropriado dentro da organização;

- Comunique de forma clara sobre como solicitar o acesso aos dados pessoais tratados por sua organização.

Dos pedidos de acesso aos dados pessoais tratados:

- Ao receber um pedido de acesso aos dados pessoais tratados por sua organização registre a data de recepção e confirme a identidade do solicitante ao direito de acesso à informação;

- A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular, no prazo de até 15 (quinze) dias, contado da data do requerimento:
  - em formato simplificado, imediatamente;
  - ou por meio de declaração clara e completa, que indique:
    - a origem dos dados;
    - a inexistência de registro;
    - os critérios utilizados e a finalidade do tratamento (observados os segredos comercial e industrial).

- As informações e os dados deverão ser fornecidos, a critério do titular, por meio eletrônico, seguro e idôneo ou sob forma impressa;

- E quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

Princípio V - Da Qualidade dos Dados

Art. 6º, Inciso V - qualidade dos dados: garantia aos titulares de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

Como atingir os objetivos desse princípio?

Você deve manter os dados pessoais dos titulares precisos, completos e atualizados, suficientemente para as finalidades para as quais serão tratados, tomando todas as medidas razoáveis para garantir que os dados pessoais que você trata não estejam incorretos.

- Certifique-se de que os dados pessoais estão precisos, completos e atualizados, o suficiente para atingir as finalidades para as quais estão sendo tratados;

- Mantenha em nível suficiente a rotina de atualização dos dados pessoais para poder cumprir as finalidades para as quais foram coletados;

- Certifique-se de que os dados pessoais são suficientemente precisos, completos e atualizados para minimizar a possibilidade de que dados inadequados possam ser usados para tomar uma decisão sobre o titular;

- Determine os limites mínimos e máximos necessários em relação à qualidade dos dados:
  - os dados pessoais devem ser atualizados apenas quando a atualização é necessária para cumprir as finalidades para as quais foram coletados e serão tratados;
  - tenha em mente que dados íntegros e exatos são essenciais nos casos em que o uso de dados pessoais imprecisos, incompletos ou desatualizados puderem influenciar negativamente decisões sobre um titular de dados, especialmente quando podem prejudicá-los;
  - avalie a importância da exatidão e da integridade em circunstâncias em que os dados são utilizados em uma base de dados de fluxo contínuo;
  - considere se sua organização pode dispor aos próprios titulares adotar para si a responsabilidade de corrigir ou atualizar seus próprios dados pessoais.

- Estabeleça uma Política de Qualidade dos Dados;

- Certifique-se de que a sua estrutura de Governança de Dados Pessoais inclui procedimentos que especifiquem:
  - os tipos de dados pessoais que precisam ser atualizados rotineiramente para exatidão e integridade;
  - quando justificado, requisitos, horários e procedimentos para uma rotina de verificação quanto à exatidão dos dados pessoais tratados, visando suas atualizações;
  - requisitos para salvar as atualizações recebidas, bem como os procedimentos para verificar a exatidão, integridade das informações prestadas;
  - como os clientes podem discordar da exatidão e integridade dos seus dados pessoais e como podem alterar suas informações, em atenção ao “Princípio do Livre Acesso”;
  - limites claros para o controle de qualidade dos dados, bem como requisitos e fundamentação para qualquer informação pessoal que sua organização:
    - utiliza ou divulga em uma base contínua, mas não tem a intenção de manter precisa e atualizada;

    - espera que clientes corrijam e/ou atualizem por conta própria.
- Declare seus controles de qualidade e deixe-os disponíveis ao público, de acordo com o "Princípio da Transparência".

Princípio VI - Da Transparência

Art. 6º, Inciso VI - transparência: garantia aos titulares de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

Como atingir os objetivos desse princípio?

Você deve ser claro e transparente com os titulares dos dados pessoais sobre como e quais dados serão tratados.

- Deixe claras, visíveis e facilmente acessíveis suas políticas de governança de dados e políticas de privacidade;
- Descreva em suas políticas:
    - quem são os agentes de tratamento, quais são as características do tratamento, com informações claras, precisas e facilmente acessíveis aos titulares de dados;
    - procedimentos para quem as reclamações ou pedidos de informação possam ser encaminhadas;
    - uma descrição de como obter acesso aos dados pessoais que sua organização trata;
    - uma descrição de quais dados pessoais são tratados;
    - uma descrição de quais agentes ou organizações você compartilha dados pessoais.
- Torne a informação disponível e desenvolva conteúdos em diversas plataformas, para dar acesso, tanto quanto possível, a todos os titulares dos dados, independentemente de suas limitações;

- Verifique se sua política de privacidade abrange todas as possibilidades de usos e divulgações de dados pessoais tratados, no seu *website*, tomando medidas adequadas para notificar os usuários de sites de todas as informações

coletadas on-line por sua organização ou por terceiros, notadamente o uso de *"cookies"* ou outras ferramentas de monitoramento não visíveis, esclarecendo tais práticas em termos compreensíveis;

- Comunique:
  - quem é seu encarregado de dados pessoais;
  - o encarregado de dados pessoais é a pessoa a quem o público pode dirigir reclamações ou pedidos de informações sobre as práticas de gestão de dados pessoais da sua organização;
  - sobre como os titulares de dados pessoais podem fazer reclamações, a respeito da violação de privacidade, à sua organização;
  - sobre como as pessoas podem ter acesso aos dados pessoais tratados por sua organização;
  - descrevendo os tipos de dados pessoais que você coleta, armazena e trata e transmite a terceiros;
  - a razão pela qual você usa ou divulga dados pessoais (caso isso se aplique);
  - demais normas, padrões ou códigos pertinentes.

- Como uma prática recomendada, inclua instruções sobre como clientes podem retirar seu consentimento (caso isso se aplique como base legal de tratamento). Inclua essas instruções como prática habitual em qualquer documento utilizado para notificar os clientes de finalidades secundárias opcionais;

- Certifique-se de que sua comunicação acerca das políticas de tratamento de dados pessoais e de privacidade são de fácil compreensão para o público em geral;

- Forneça aos titulares dos dados pessoais ferramentas para que eles possam visualizar como sua organização está usando seus dados e se as políticas estão sendo adequadamente aplicadas.

Princípio VII - Da Segurança

Art. 6º, Inciso VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Como atingir os objetivos desse princípio?

Você deve garantir que possui as medidas de segurança apropriadas para proteger os dados pessoais tratados.

- Proteja os dados pessoais utilizando técnicas administrativas e organizacionais de segurança apropriadas;

- Proteja os dados pessoais, independentemente do formato em que são tratados: físicos ou digitais;

- Proteja os dados pessoais contra perda ou roubo, destruição, bem como acesso não autorizado, divulgação, cópia, uso ou modificação;

- Conscientize o time da importância de manter a confidencialidade dos dados pessoais;

- Bloqueie o acesso não autorizado ao destruir ou eliminar dados pessoais;

- Proteja os dados pessoais sensíveis com um nível mais elevado de proteção;

- Inclua entre os seus métodos de proteção e segurança:
  - medidas físicas, tais como armários e arquivos trancados com acesso restrito, inclusive às áreas em que não se possa garantir total segregação física e lógica de time não autorizado;
  - medidas organizacionais, tais como permissões de segurança e limite/ segregação de acesso físico e lógico aos dados pessoais;
  - medidas tecnológicas, como o uso de senhas e criptografia.

- Estabeleça uma Política Informativa de Segurança:
  - reveja suas práticas atuais de segurança da informação, políticas e sistemas para determinar se a sua organização está cumprindo com as responsabilidades descritas acima;
  - adote as medidas apropriadas, tais como as descritas na ISO 27002, para corrigir eventuais deficiências;
  - desenvolva e implemente uma política, ou atualize as já existentes, consolidando suas práticas de segurança e procedimentos de acordo com o "Princípio da Segurança". Inclua a exigência e procedimentos para

documentar e acompanhar as violações de segurança, informando aos indivíduos afetados.

- Certifique-se de que sua política aborda as seguintes responsabilidades:
  - salvaguardas físicas:
    - implemente medidas físicas, conforme a necessidade, para garantir a segurança de acesso físico e lógico aos dados pessoais, incluindo:
      - armários bloqueados;
      - política de mesa limpa;
      - acesso restrito aos dados pessoais;
      - instalações (escritórios, salas, estabelecimentos) seguras;
      - sistemas de alarme e monitoramento.
    - certifique-se de que as salvaguardas físicas são adequadas para:
      - o tipo de dados pessoais tratados (por exemplo, um nível mais elevado de proteção para dados sensíveis);
      - o modo e a extensão da distribuição ou transmissão;
      - formato (por exemplo, papel ou arquivos eletrônicos);
      - métodos de armazenamento.
    - certifique-se de que as salvaguardas físicas são suficientes para proteger contra perda ou roubo, e contra o acesso não autorizado, divulgação, cópia, uso, modificação, deleção ou destruição.

  - salvaguardas organizacionais:
    - implementar medidas organizacionais necessárias para garantir a segurança de acesso aos dados pessoais, incluindo:
      - autorização e limite ao acesso em uma base de “finalidade do acesso”;
      - autorizações de segurança e classificações;
      - acordos de confidencialidade;
      - procedimentos de segurança específicos;
      - treinamento de segurança da informação;
      - monitoramento interno regular dos sistemas de segurança da informação;
      - monitoramento independente de auditoria de sistemas de segurança da informação.
    - certifique-se de que suas salvaguardas organizacionais são adequadas para:
      - o tipo de dados pessoais (sensível ou não);
      - a quantidade de informações armazenadas;

        - o modo e a extensão da distribuição ou transmissão dos dados pessoais;
        - formato (por exemplo, papel ou arquivos eletrônicos);
        - métodos de armazenamento.
    - certifique-se de que suas salvaguardas organizacionais são suficientes para proteger contra perda ou roubo, e contra o acesso não autorizado, divulgação, cópia, uso e modificação.

- salvaguardas tecnológicas
    - implementar medidas organizacionais necessárias para garantir a segurança de acesso aos dados pessoais, incluindo:
        - requisitos de identificação (especialmente para transações *online*) para estabelecer legítima identidade para acessar os dados pessoais;
        - autenticação (ou seja, senhas ou outros identificadores exclusivos para assegurar autorização de acesso aos dados pessoais);
        - controles de acesso ao sistema;
        - canais seguros para transmissões de dados pessoais, tal como VPN;
        - criptografia de dados para armazenamento e transporte;
        - *firewalls* e procedimentos para detecção de intrusão;
        - trilhas de auditoria automáticas para sistemas de processamento de dados pessoais;
        - controles de manutenção, incluindo registros e gestão de mudança;
        - registros transacionais e logs.
    - certifique-se de que as salvaguardas tecnológicas são adequadas para:
        - o tipo de dados pessoais, como por exemplo sensível ou não, dados financeiros ou outros que possam expor negativamente o titular ou gerar discriminação;
        - as quantidades e tipos de dados armazenados;
        - a forma e a extensão da distribuição ou transmissão.
    - certifique-se de que as salvaguardas tecnológicas (independentemente do uso de tecnologia, com ou sem fio) são suficientes para proteger contra perda ou roubo, acesso não autorizado, divulgação, cópia, uso, modificação, deleção ou destruição;

- conscientização do time:
    - defina limites apropriados para o acesso dos colaboradores aos dados pessoais mantidos por sua organização;

- como regra geral, conceda a autorização para acesso aos dados pessoais em uma "finalidade do acesso", por exemplo, acesso necessário para desempenhar funções de trabalho pré-definidas e autorizadas;
- especifique quem está autorizado a acessar e manipular os dados pessoais mantidos por sua organização;
- conscientize seu time da importância da privacidade e proteção de dados pessoais;
- quando a informação pessoal é sensível ou caso as consequências potenciais de divulgações impróprias são significativas, use acordos de confidencialidade com os trabalhadores;
- treine sua equipe em políticas e procedimentos para a sua organização manter a segurança e a confidencialidade dos dados pessoais;
- realize treinamentos regulares para garantir a sensibilização contínua e a segurança no tratamento de dados pessoais por parte do time.

- eliminação segura:
  - utilize procedimentos seguros para a eliminação ou destruição de dados pessoais, bem como equipamentos ou dispositivos utilizados e reutilizados (formatados, inutilizados) para o armazenamento de dados pessoais;
  - ao descartar ou destruir dados pessoais, tome as medidas adequadas para evitar que pessoas não autorizadas tenham acesso ao material a ser destruído;
  - quando da eliminação de equipamentos ou dispositivos utilizados para o armazenamento de dados pessoais (tais como armários de arquivo, computadores e fitas de *backup*), tomar as medidas adequadas para remover ou excluir qualquer informação armazenada ou, de outra forma, para impedir o acesso por pessoas não autorizadas. HDs, *pendrives* e até mesmo memórias RAM são passíveis de conter dados pessoais mesmo após suas respectivas formatações.

- teletrabalho, trabalho volante e *homeoffice*:
  - desenvolva procedimentos formais para que os colaboradores removam dados pessoais de seus dispositivos enquanto estiverem fora da sua organização. Analise os riscos de segurança particulares que estas situações criam e desenvolva soluções para limitar os riscos.

Princípio VIII - Da Prevenção

Art. 6º, Inciso VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Como atingir os objetivos desse princípio?

Você deve adotar medidas técnicas e organizacionais apropriadas para prevenir danos em virtude de tratamento de dados pessoais, antes mesmo de iniciar a coleta, ou seja, ocupar-se com privacidade e proteção de dados *by design* e *by default*.

- Considere antecipadamente os problemas de proteção de dados e privacidade em tudo o que você faz, desde a concepção de um processo, serviço ou produto;
- Considere e integre a proteção de dados e a privacidade em suas atividades de tratamento de dados pessoais, práticas de negócios e processos internos;
- Torne a proteção de dados um componente essencial da funcionalidade do núcleo de seus sistemas, produtos e serviços com tratamento de dados pessoais;
- Preveja riscos e eventos invasivos à privacidade antes que eles ocorram e tome medidas para evitar danos aos titulares de dados pessoais;
- Trate apenas os dados pessoais de que necessita para seus propósitos legítimos/finalidades declarados, tornando padrão a não coleta de dados úteis ou não declarados nos propósitos iniciais, os quais podem ser autorizados/consentidos ou fornecidos como opção do titular;
- Ocupe-se em proporcionar salvaguardas para proteção automática de dados pessoais em qualquer sistema de TI, serviço, produto e/ou prática comercial, para que os titulares não precisem adotar nenhuma ação específica para proteger sua privacidade;
- Ofereça padrões de privacidade fortes, opções e controles fáceis de usar e respeite as preferências do usuário;

- Quando usar sistemas não proprietários, serviços ou produtos em suas atividades de tratamento de dados pessoais, verifique se utilizam apenas aqueles cujos designers e fabricantes levam em consideração questões de privacidade e proteção de dados.

Princípio IX - Da Não Discriminação

Art. 6º, Inciso IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

Como atingir os objetivos desse princípio?

Você deve adotar medidas técnicas e organizacionais apropriadas para proteger direitos da personalidade, promovendo igualdade material, evitando qualquer estigmatização baseada no tratamento de seus dados pessoais, em razão de sua classificação e segmentação.

- Evite modelar arquitetura de tratamento de dados, por meio de filtros que estigmatizam, criam estereótipos ou segregam determinadas categorias de titulares, limitando a atuação destes usuários e/ou forçando-os a determinadas condutas.

Princípio X - Da Responsabilização e Prestação de Contas

Art. 6º, Inciso X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Como atingir os objetivos desse princípio?

Você deve assumir a responsabilidade pelo que faz com os dados pessoais e como cumpre os princípios da LGPD, adotando medidas e registros apropriados para poder demonstrar sua conformidade.

- Aceite a responsabilidade por dados pessoais sob sua posse ou custódia;

- Proteja todos os dados pessoais na posse ou custódia da organização, incluindo dados que foram transferidos para um terceiro para tratamento e/ou recebidos de um terceiro para tratamento;
- Use meios contratuais para garantir um nível apropriado de proteção enquanto os dados pessoais estão sendo tratados por sua organização ou por terceiros (operadores);

- Desenvolva e implemente políticas e práticas para apoiar os 10 princípios estabelecidos no Art. 6º da LGPD, incluindo:
  - implementação de procedimentos para proteção de dados pessoais;
  - o estabelecimento de procedimentos (*playbook*) para receber e responder às consultas e reclamações dos titulares, investigações e processos administrativos da ANPD;
  - treinamento de pessoal e comunicação de informações ao time de colaboradores sobre a organização das políticas e boas práticas de Governança de Dados Pessoais.

- Nomeie pelo menos uma pessoa na organização ou terceira pessoa jurídica com essa finalidade, para ser o encarregado de dados pessoais (*Data Privacy Officer*), bem como para evangelização das políticas e boas práticas. Se essa pessoa não é um encarregado (*Data Privacy Officer*) dedicado, garanta que a descrição do trabalho inclua a responsabilidade de manejar as boas práticas exigidas por lei. Essa pessoa deve:
  - ser um tomador de decisão, que é claramente apoiado em seu papel, pela alta administração, em promover a privacidade como um valor corporativo;
  - ser capaz de intervir em questões de privacidade em toda a organização, quando necessário;
  - orientar a organização para que os recursos sejam suficientes e adequados para a implementação de políticas de privacidade e gestão

de riscos de privacidade, garantindo avaliações periódicas para que seu cumprimento esteja em conformidade com a LGPD;
    - demonstrar total conhecimento sobre os dados pessoais que a organização trata, suas políticas e procedimentos;
    - demonstrar total conhecimento das responsabilidades da organização em relação à LGPD e em relação às demais normas legais ou infralegais que definem regras para tratamento de dados pessoais para sua organização;
    - explicar os procedimentos de pedido de informação e de queixas;
    - realizar ou supervisionar investigações de reclamações.

- sempre que necessário, publique o nome ou título e endereço comercial do encarregado de dados (*Data Privacy Officer*), interna e externamente;

- desenvolva orientações que irão ajudar a equipe a responder a perguntas do encarregado de dados pessoais (*Data Privacy Officer*) sobre o seu programa de privacidade, incluindo informações sobre como entrar em contato com o encarregado de dados, se estas o solicitarem.

- Treine seu time, em especial, mas não exclusivamente, de nível gerencial, bem como mantenha-os informados, de modo que possam responder perguntas sobre políticas e práticas de privacidade e proteção de dados da sua organização:
    - para qual finalidade sua organização coleta dados pessoais;
    - nos casos de utilização da base legal "Consentimento" explicar aos titulares de dados quando e como eles podem retirar seu consentimento e quais as consequências, caso existam, podem advir de tal retirada;

- Mantenha seu time informado sobre novas questões de privacidade levantadas pelas mudanças tecnológicas, reclamações públicas de titulares de dados pessoais, decisões dos tribunais, da ANPD;

- Desenvolva/adquira um sistema e/ou implemente um processo interno para monitorar a conformidade da sua organização com a LGPD e demais normas legais e infralegais, com mapeamento contínuo e monitoramento do ciclo de vida dos dados pessoais;

- Defina políticas administrativas para governança e gerenciamento do ciclo de vida dos dados pessoais contendo:

- estruturas organizacionais, funções e responsabilidades para atingir os requisitos da LGPD;
- procedimentos e requisitos para reportar à alta administração (*C-Level*) as políticas de privacidade e procedimentos de gestão de risco;
- atribuição de recursos suficientes e apropriados para implementar e apoiar políticas de privacidade;
- procedimentos e requisitos para realizar avaliações de impacto de privacidade e proteção de dados:
  - antes de ofertar novos produtos ou serviços;
  - quando novos sistemas e processos são introduzidos;
  - quando sistemas e processos já existentes são significativamente alterados.

- informações sobre padrões de segurança e de gestão para assegurar que os dados pessoais estejam salvaguardados contra a sua divulgação não autorizada, modificação, interrupção de acesso, remoção ou destruição;

- procedimentos e requisitos para a revisão periódica do *design*, aquisição, desenvolvimento, implementação, configuração e gerenciamento de infraestrutura, sistemas, aplicativos e sites para assegurar a coerência com as políticas e procedimentos de privacidade;

- procedimentos e requisitos para identificação, avaliação e elaboração de relatórios para corrigir as causas de violações de privacidade, incluindo a perda de dados pessoais ou o seu uso inadequado;

- procedimentos e requisitos para resposta às reclamações de privacidade, bem como para realizar ações corretivas, suspensivas e de deleção dos dados pessoais por solicitação do titular dos dados pessoais;

- procedimentos e requisitos para treinamentos periódicos sobre privacidade e proteção de dados para o time;

- auditoria de conformidade para controle de boas práticas e Governança de Dados Pessoais.

- Defina uma Política de Privacidade que se aplique a toda organização, decupada

e complementada por normas que se aplicam às áreas de negócio específicas, se necessário;

- Comunique suas políticas e práticas de coleta e uso de dados pessoais e os passos que os titulares de dados pessoais podem tomar para protegê-los, exercendo seu direito fundamental à privacidade:
  - desenvolva e dissemine informações (informativos, flyers, folhetos, sites ou outros materiais escritos) para explicar, em linguagem simples, as políticas de privacidade e proteção de dados da sua organização, bem como práticas e procedimentos para os clientes e para o público em geral;
  - certifique-se de que, utilizando essas informações, os titulares de dados possam:
    - obter acesso aos seus dados pessoais;
    - corrigir seus dados pessoais;
    - fazer perguntas sobre as políticas ou práticas de privacidade da sua organização;
    - reclamar sobre políticas ou práticas de privacidade da sua organização.
  - para seus clientes em particular, torne mais fácil descobrir com quem na organização o titular de dados deve entrar em contato, a fim de:
    - fazer perguntas sobre seus dados pessoais;
    - solicitar o acesso aos seus dados pessoais;
    - corrigir seus dados pessoais.

Organizações podem transferir dados pessoais a terceiros para tratamento em razão de uma variedade de motivos legítimos. É importante notar que a organização que decide sobre os dados mantém o controle - por isso é denominada controlador - em relação às possibilidades de tratamento, incluindo temporalidade e finalidades, mas divide a responsabilidade com o terceiro, denominado operador. As melhores práticas de transferência de dados pessoais para terceiros incluem:

- Cláusulas de proteção de privacidade e proteção de dados em contratos, para assegurar que terceiros, a quem os dados pessoais são transferidos para tratamento, forneçam o mesmo nível de proteção e conformidade com a legislação vigente, na mesma medida que sua organização faz;
- Garanta que o terceiro:
  - nomeie uma pessoa para lidar com todas as questões de privacidade e proteção de dados relacionadas com os dados pessoais transferidos;

- Garanta que o terceiro:
  - nomeie uma pessoa para lidar com todas as questões de privacidade e proteção de dados relacionadas com os dados pessoais transferidos;
  - limite o uso dos dados pessoais para fins expressamente autorizados pela sua organização;
  - limite expressamente o acesso físico e lógico aos dados pessoais;
  - encaminhe, em prazo expressamente determinado, qualquer solicitação do titular de dados pessoais, seja para acesso, modificação suspensão de tratamento, exclusão, portabilidade, bem como queixas a respeito do tratamento, ao encarregado de dados pessoais, da sua organização;
  - utilize medidas de segurança apropriadas para proteger os dados pessoais transferidos;
  - retorne ou elimine com segurança todas as informações transferidas após a conclusão do contrato ou de cada etapa do contrato previamente estabelecida;
  - emita relatórios sobre a adequação dos dados pessoais transferidos, contendo medidas de segurança e controles, bem como permita que sua organização possa auditar o seu cumprimento, se necessário.

4 Parte 2: Checklist de Autoavaliação

Importância da Autoavaliação

Uma boa gestão do ciclo de vida do dado pessoal está intimamente ligada à reputação de uma organização, sua marca, relações negociais, responsabilidade legal, fidelização de clientes/usuários, valorização dos colaboradores, crescimento dos negócios e principalmente lealdade com seus *stakeholders*. A autoavaliação é, em última análise, do interesse particular de uma organização que deseja ser o melhor possível para a sociedade, perpetuando sua atuação.

Essa ferramenta de autoavaliação deve ser aplicada como parte de um programa de privacidade e proteção de dados bem estruturado, seja ele ou não um Programa de Governança de Dados Pessoais, denominação que a Fundacred optou adotar. Autoavaliações feitas de forma periódica são ferramentas valiosas que ajudam uma organização a endereçar e resolver problemas em seus processos internos, melhorando a proposta de valor e, por conseguinte, sua entrega e sua oferta.

O presente *checklist* deve ser constantemente atualizado com novas situações identificadas em sua organização.

Como se Preparar Para a Autoavaliação

Este exercício voluntário de autoavaliação implica não só garantir que controles de privacidade e proteção de dados foram desenvolvidos, mas também coletar evidências de que esses controles foram efetivamente implementados. Quanto mais evidências sobre o cumprimento por parte da sua organização, você será capaz de identificar melhor e avaliar os riscos de privacidade e proteção de dados.

A autoavaliação é capaz de identificar fraquezas e ameaças sujeitas a um plano de ação apropriado, mas precisa ser bem executada, a fim de ser bem sucedida. Ela vai exigir tempo e recursos para ser concluída. A organização deve estar preparada para considerar os resultados da avaliação, investir em treinamentos adequados e ações para lidar com riscos inaceitáveis, além de reforçar as suas capacidades de proporcionar um bom nível de Governança de Dados Pessoais.

Existem algumas atividades preparatórias que facilitam o exercício de autoavaliação. Todas elas, por si só, ajudarão a reduzir as lacunas de informações durante o preenchimento do *checklist*. Essas atividades incluem: a avaliação do seu modelo de negócio; a realização de um inventário de dados pessoais; a realização de um mapeamento do ciclo de vida dos dados pessoais e a revisão de políticas, processos internos e procedimentos.

Recomendamos a assessoria de um time tecnicamente habilitado para a realização das atividades descritas acima.

A exigência de time técnico habilitado dá-se pela complexidade, por exemplo, de realizar inventário de dados pessoais - estruturados (a exemplo do banco de dados) e não estruturados (exemplos: *hardwares* de usuários e caixas de e-mail) por área de negócio que será envolvida no exercício de avaliação.

Embora possamos utilizar tabelas simples para criar um inventário sobre o tipo de dados pessoais coletados e tratados e onde são mantidos dentro da organização, localizá-los em banco de dados estruturados e em ambientes não estruturados requer esforço técnico importante. Por exemplo, o inventário pode identificar

o nome de um aplicativo, como o PeopleSoft, a série de arquivos impressos ou digitais dentro do aplicativo (arquivos de pessoal de RH, remuneração e benefícios, arquivos de avaliações). O inventário deve descrever os tipos de dados pessoais (registros médicos, financeiros), como são coletados, utilizados, divulgados, mantidos, eliminados ou armazenados.

Dependendo do número de processos internos e sistemas de informação dentro de sua organização, envolvidos na coleta, processamento ou transferência de dados pessoais, esta tarefa pode tornar-se bastante complexa.

Na Fundacred, começamos com um projeto piloto em uma escala mais gerenciável, um modelo *lean*, para poder testar a dinâmica e aprender com as dificuldades enfrentadas.

Uma boa forma de entender o ciclo de vida do dado pessoal de uma organização é desenvolver diagramas de processos de negócios para cada grande atividade organizacional que está sendo avaliada, demonstrando um fluxo de alto nível do ciclo de vida dos dados pessoais em processos ponta-a-ponta. Na Fundacred utilizamos a anotação técnica BPMN (*Business Process Model and Notation*), o que nos proporciona agilidade na tomada de decisão quanto ao redesenho de processos, com base nos ciclos de vida dos dados pessoais.

Recomendamos, ainda, que todo o trabalho seja realizado por comitês interdisciplinares (com uma mesma visão para alcançar a mesma eficácia) e multidisciplinares (para que atuem conjuntamente, mas realizando suas atividades isoladamente) para preservar suas regras de negócio enquanto mapeiam os processos.

O objetivo desse *Framework Multistakeholder* que a Fundacred está disponibilizando é promover reflexões importantes para que sejamos, todos, capazes de, constantemente, responder às seguintes perguntas:

1. **Como a LGPD define dados pessoais e como essa definição aplica-se no contexto da minha organização?**

2. **Quais dados pessoais minha organização coleta?**

3. **Quais dados pessoais minha organização trata, mas não coleta diretamente?**

4. **Por que coletamos e tratamos dados pessoais?**

5. **Quem na organização coleta dados pessoais?**

6. **Quem na organização tem acesso a dados pessoais?**

7. **Onde armazenamos dados pessoais?**

8. **Em que formatos armazenamos dados pessoais (por exemplo, digital, papel, fita de áudio/vídeo, armários)?**

9. **Como podemos manter os dados pessoais seguros?**

10. **Que dados pessoais divulgamos ou transferimos para outras organizações e pessoas, e por quê?**

11. **Para que outras organizações vamos divulgar ou transferir dados pessoais e como elas vão utilizar esses dados?**

12. **Por quanto tempo vamos manter os dados pessoais?**

13. **Quanto tempo é necessário manter dados pessoais?**

14. **Quando e como vamos descartar dados pessoais?**

Utilizando a Ferramenta

Essa ferramenta será mais eficiente quando seu programa de governança de dados já estiver implantado e implementado, estiver em funcionamento por tempo suficiente para que você possa verificar a sua eficácia. Todavia, estas listas de verificação permitirão, desde já, que você avalie o quão perto sua organização está do ponto ótimo em relação aos princípios da LGPD, para que possa começar agora a mudança necessária nos seus processos e, em algumas situações, até mesmo na sua oferta.

Cada pergunta exige que você descreva a evidência sobre a qual a avaliação se baseou, bem como eventuais circunstâncias atenuantes para explicar todas as respostas que constam "não atende". As evidências devem ser suficientes para que a avaliação seja significativa e, eventualmente, transformadora. Você deve descrever como tratará os dados pessoais para atender cada objetivo, seja por meio de políticas, avisos, procedimentos, processos, estruturas e/ou valores organizacionais.

Há dois aspectos para compreender o quão bem um mecanismo de "Governança de Dados Pessoais" está sendo empreendido:

1. O Programa de Governança de Dados Pessoais precisa ter sido adequadamente projetado para atender às exigências da legislação atinente ao seu modelo de negócio (não se limite à LGPD, atente-se às demais normas, especialmente às regulações do seu setor/mercado);

2. O Programa de Governança de Dados Pessoais precisa funcionar como previsto, ou seja, seu time precisa seguir de forma consistente a política estabelecida no programa.

Você não pode se considerar em conformidade com a LGPD e com os demais dispositivos legais já citados, até que tenha avaliado seus processos e seus mecanismos de controle, bem como se tais mecanismos estão realmente sendo observados no ambiente de negócios.

Recomendação importante: lembramos que essa autoavaliação, assim como toda a ferramenta que estamos disponibilizando, não substitui o trabalho de uma assessoria especializada, a qual recomendamos a contratação, minimamente contendo profissionais de Segurança da Informação e advogados com experiência em Privacidade e Proteção de Dados Pessoais.

Interpretação dos Resultados da Autoavaliação

Um Programa de Governança de Dados Pessoais maduro é caracterizado por uma documentação clara acerca da compreensão e mitigação de riscos, pela diligência nas decisões que devem colaborar para definir prioridades em relação às medidas corretivas, oportunizando, assim, a concepção de um cronograma realista para sua evolução.

Você deve considerar cuidadosamente os riscos envolvidos em qualquer área onde sua organização tiver lacunas importantes em relação à conformidade. Lembre-se que uma única ação corretiva pode endereçar o alcance de múltiplos objetivos, por isso, é importante decidir, implantar e acompanhar a execução de ações corretivas e cada um dos impactos positivos que irão sanar deficiências encontradas com essa avaliação.

Após analisar os resultados da autoavaliação, você deverá permitir que sua organização dedique recursos para melhorar as práticas de governança de dados pessoais. Analise os resultados da autoavaliação para compreender se existem princípios específicos contra os quais sua organização exibe fraquezas e em qual nível de maturidade sua organização se encontra.

É muito importante que, durante a autoavaliação, você registre processos e eventos que geram riscos de privacidade e proteção de dados. Na seção a seguir eles serão abordados de forma mais detalhada.

Antes de divulgar internamente os resultados de sua autoavaliação, tenha em mente revisitar com cada área e/ou unidade de negócio, os resultados observados. Documente quaisquer circunstâncias que causaram um mau resultado para que sejam tratadas de forma objetiva pelas áreas e/ou unidades de negócio de sua organização.

Um programa de governança de dados pessoais amadurece com o tempo, por isso, a avaliação de conformidade da sua organização deve ser colocada no contexto desta curva de maturidade. Ao avaliar o seu programa em relação às melhores práticas, considere uma escala que vai ter relevância em toda a organização. A escala de maturidade também deve ser flexível o suficiente para ser aplicada para várias áreas e/ou unidades de negócios e *stakeholders* de sua organização.

Você pode considerar a seguinte escala para avaliar os resultados totais de cada princípio visitado:

Maturidade Nível 1	Inexistente / Avaliação não desenvolvida (Não Atende)
Maturidade Nível 2	Estágios iniciais de desenvolvimento (Atende Parcialmente)
Maturidade Nível 3	Avançado (Atende Parcialmente com possíveis melhorias)
Maturidade Nível 4	Totalmente desenvolvido (Atende) - Requisitos atingidos de forma consistente - apenas pequenos ajustes ou nenhum ajuste necessário.

Avaliação de Impacto e Plano de Ação:

Durante a autoavaliação, você possivelmente identificará eventos que geram riscos de privacidade e proteção de dados na sua organização. É muito importante que você registre esses eventos, áreas ou unidades de negócio, bem como seus processos relacionados.

"Risco de Privacidade e Proteção de Dados" é o potencial de vulnerabilidades que uma determinada ameaça pode gerar em relação a:

- um ativo que contém dados pessoais;
- e/ou um processo de negócio envolvendo dados pessoais que pode causar, mesmo que de forma não intencional, acesso, modificação ou danos (deleção total ou parcial) a dados pessoais.

Os riscos podem ser em relação à sua organização, seus clientes, time, fornecedores e demais *stakeholders*.

O impacto, ou gravidade do risco, é proporcional à sua probabilidade estimada de ocorrência e o impacto potencial para a sua organização, ou individualmente, a um titular de dados pessoais.

A avaliação de impacto é a identificação e análise de riscos relevantes à privacidade e proteção de dados. Você pode utilizar essa base de informações para endereçar como esses riscos serão geridos, incluindo medidas que devem ser implementadas para reduzi-los a um nível aceitável.

Priorize as deficiências em seu Programa de Governança de Dados Pessoais e crie um plano de ação. Áreas e/ou unidades de negócio não conformes podem ser classificadas por meio da realização de um processo de avaliação de risco de privacidade:

- Identifique todos as repostas que constam “não atende” ou “parcialmente atendidas” em sua autoavaliação e sinalize-as para revisão;

- Considere priorizar os planos de ações que tiverem respostas que constam “não atende” ou “atende parcialmente” em que as implicações potenciais (ocorrências e suas probabilidades de impacto) sejam de impacto “extremo” e probabilidade “quase certo”, atacando as de impacto menor e probabilidade de ocorrência menor sucessivamente;

- Se você tem parcial ou nenhum controle sobre o processo negocial avaliado, use as informações a partir do seu conhecimento sobre a organização para determinar quão provável é que este evento adverso ocorrerá, e o possível impacto decorrente;

- A seguir, uma sugestão de escala que você pode usar para avaliar esses fatores para cada um dos objetivos identificados como deficientes:

PROBABILIDADE DE OCORRÊNCIA		
Nível	**Descritor**	**Descrição**
5	**Quase certo**	Evento ocorre regularmente nesse processo negocial, área ou unidade de negócio em que estou.
4	**Provável**	O evento ocorreu nesse processo negocial, área ou unidade de negócio em que estou mais de uma vez ou está ocorrendo em minha organização em circunstâncias semelhantes.
3	**Moderado**	O evento já ocorreu antes nesse processo negocial, área ou unidade de negócio em que estou ou foi observado em circunstâncias semelhantes.
2	**Improvável**	O evento ocorreu com pouca frequência em outro processo negocial, área ou unidade de negócio, em circunstâncias semelhantes, mas não ocorreu onde estou.
1	**Raro**	Evento quase nunca foi observado; pode ocorrer apenas em circunstâncias excepcionais.

IMPACTO		
Nível	**Descritor**	**Descrição**
1	**Extremo**	Um grande evento com potencial para provocar danos de longo prazo, comprometendo a capacidade da organização de cumprir seus objetivos. As consequências poderiam causar sérios problemas de regulação, de reputação, financeiras ou operacionais, de longo prazo para a organização, exigindo intervenção da alta gestão (C-Level). O evento também poderia causar ao titular de dados pessoais riscos e/ou danos significativos à sua reputação, danos financeiros e/ou sofrimento emocional pela violação de sua privacidade.
2	**Muito alto**	Um evento crítico que, com uma gestão adequada, pode ser suportado pela organização. As consequências de um evento como esse poderia incluir preocupações regulatórias, de reputação, financeiras ou operacionais significativas para a organização, e exigem intervenção da alta gestão (C-level). O evento também poderia causar ao titular de dados pessoais riscos e/ou danos significativos à sua reputação, danos financeiros e/ou sofrimento emocional pela violação de sua privacidade.

3	**Médio**	Um evento significativo que pode ser gerido em circunstâncias normais pela organização. As consequências podem causar problemas de regulação, de reputação, financeiras ou operacionais, mas pode ser gerenciado internamente pela organização. Esta categoria também pode resultar em consequência moderada para o indivíduo, tais como a exposição de algumas informações financeiras, como, por exemplo, salário. Não há impacto que acarrete risco ou dano relevante para o titular de dados pessoais e o incidente pode ser contido dentro da organização sem exposição.
4	**Baixo**	Um evento em que as consequências podem ser absorvidas, mas o esforço de gestão é necessário para minimizar o impacto. As consequências poderiam ameaçar a conformidade com normas regulamentares, reputação e a própria operação, mas seria tratado internamente. O evento seria de baixa consequência para a organização. Não há impacto que acarrete risco ou dano relevante para o titular de dados pessoais e o incidente pode ser contido dentro da organização, sem exposição.
5	**Desprezível**	Um evento, em que as consequências podem ser absorvidas pela atividade. As consequências poderiam ameaçar normas regulamentares, reputação e/ou a própria operação, mas pode ser tratado internamente. Isso seria de baixa consequência para a organização. Não há impacto que acarrete risco ou dano relevante para o titular de dados pessoais e o incidente pode ser contido dentro da organização, sem exposição.

Classificação dos Resultados da Sua Avaliação de Risco

Se a ocorrência de um evento adverso é provável (por exemplo, você sabe que a sua organização coleta rotineiramente dados pessoais não essenciais para a consecução do negócio e você não tem controles para lidar com eles) e o impacto também é significativo (onde, por exemplo, você vislumbra danos para a sua credibilidade e para sua marca), você deve dar mais atenção a essas deficiências do que as que geram menor probabilidade de ocorrência e um menor impacto.

Trace os resultados desta classificação em um mapa de calor para entender a classificação relacionada de suas deficiências. Um gráfico com mapa de calor pode ajudar:

IMPACTO	Extremo					
	Muito alto					
	Médio					
	Baixo					
	Desprezivel					
		Raro	Improvável	Moderado	Provável	Quase certo
		PROBABILIDADE				

Desenvolva ações (plano de ação) específicas para sanar todas as deficiências, reescrevendo seus processos, se necessário, para reduzir a probabilidade do evento adverso ou reduzir o impacto do evento. Em boa parte das vezes, os controles que você definir e os novos processos terão um impacto positivo sobre os dois aspectos de risco (probabilidade e impacto), pois potencialmente sanam múltiplas deficiências.

Você também pode concentrar-se primeiramente em ações que mitiguem riscos mais elevados e que são relativamente fáceis de implementar.

Lista de Verificação Para o Princípio I - Finalidade

DECLARAÇÃO	AVALIAÇÃO			EVIDÊNCIAS	PLANO DE AÇÃO
	Atende	Não atende	Atende parcialmente		
Você identifica por que está tratando dados pessoais antes ou depois da coleta.					
Você documentou seus propósitos legítimos e finalidades para tratar dados pessoais.					
Você determinou as quantidades e tipos de dados pessoais necessários para cumprir com cada finalidade ao tratar dados pessoais.					
Você determinou os motivos para os quais está coletando dados pessoais, bem como a quantidade e os tipos de dados pessoais coletados são razoáveis para os titulares de dados com os quais você se relaciona.					
Você distinguiu entre dados pessoais essenciais - para os fins negociais principais - e dados pessoais não essenciais - dados pessoais que facilitam a relação negocial, para fins secundários.					
Você identificou dados pessoais não essenciais que você trata e forneceu ao seu time orientações sobre como proceder quando os titulares optarem por não fornecer ou permitir tratamento.					
Você comunica o titular de dados antes de realizar tratamento com finalidade distinta e não compatível com a original, solicitando seu consentimento.					
Você acompanha o ciclo de vida do dado pessoal sob sua responsabilidade para descartá-lo quando e se a finalidade específica almejada for alcançada, não havendo mais justificativa jurídica para a sua manutenção.					

Lista de Verificação Para o Princípio II - Adequação

DECLARAÇÃO	AVALIAÇÃO			EVIDÊNCIAS	PLANO DE AÇÃO
	Atende	Não atende	Atende parcialmente		
Você limita a quantidade e tipo de dados pessoais que coleta para o que é necessário para a finalidade legitimamente declarada.					
Você documenta os tipos específicos de dados pessoais coletadas atrelados às finalidades fins para tratamento.					
Você registra quando coleta dados pessoais de titulares por meio de um terceiro titular de dados pessoais.					
Você não usa nem transfere dados pessoais para fins além daqueles para os quais foram coletados, exceto com o consentimento do titular ou por obrigação legal.					
Sua estrutura de governança de dados pessoais endereça questões atinentes à destruição de dados pessoais, incluindo o registro de atividades do time que executa tais serviços.					
Você possui uma política de retenção ou programações de retenção de dados pessoais, listando os tipos de dados pessoais que você possui, para que os utiliza e por quanto tempo pretende mantê-los.					

Lista de Verificação Para o Princípio III - Necessidade

DECLARAÇÃO	AVALIAÇÃO			EVIDÊNCIAS	PLANO DE AÇÃO
	Atende	Não atende	Atende parcialmente		
Você só coleta e trata dados pessoais após ter certeza de que a finalidade pretendida pode ser atingida, exclusivamente, mediante respectivo tratamento.					
Você distingue entre coleta necessária (obrigatória) e opcional de dados pessoais.					
Você só retém dados pessoais enquanto for necessário para permitir o cumprimento dos propósitos identificados e declarações de finalidades.					
Você identifica o volume mínimo necessário de dados pessoais para cumprimento dos propósitos identificados e declarações de finalidades					

Lista de Verificação Para o Princípio IV - Livre Acesso

DECLARAÇÃO	AVALIAÇÃO			EVIDÊNCIAS	PLANO DE AÇÃO
	Atende	Não atende	Atende parcialmente		
Você adota políticas e procedimentos para responder a pedidos de dados pessoais.					
Você esclarece sua equipe da importância dos pedidos expressos de acesso a dados pessoais por parte de titulares e como é o processamento desses pedidos.					
Você informa os titulares de dados pessoais sobre a existência de tratamento de seus dados pessoais no momento da coleta de um pedido escrito de acesso a dados pessoais.					
Você limita a recusa de bloqueio, suspensão, deleção e portabilidade integral de dados pessoais apenas em casos legalmente previstos.					
Você fornece os contatos de todos os terceiros a quem tenham sido transferidos os dados pessoais do titular, ou pelo menos informa os tipos de terceiros a quem esses dados são geralmente transferidos/divulgados.					
Você responde a um pedido de informações em não mais de 15 dias.					
Você fornece acesso aos dados pessoais tratados em um formato legível e que fornece esclarecimentos aos titulares a respeito do tratamento.					
Você esclarece os solicitantes das razões da recusa de atualização, alteração, suspensão de tratamento, bloqueio e deleção nos casos em que possui justificativa legal para tanto.					
Você permite que os titulares de dados reclamem a exatidão dos dados pessoais e os alterem desde que demonstrem que os dados são imprecisos ou incompletos.					

Lista de Verificação Para o Princípio V - Qualidade dos Dados

DECLARAÇÃO	AVALIAÇÃO			EVIDÊNCIAS	PLANO DE AÇÃO
	Atende	Não atende	Atende parcialmente		
Você toma medidas razoáveis para garantir que os dados pessoais sejam precisos, completos e atualizados antes de utilizá-los para tomar decisões.					
Você só atualiza dados pessoais se o procedimento é necessário para cumprir as finalidades para as quais foram coletados.					
Sua estrutura de governança de dados pessoais aborda a exatidão e a integridade dos dados pessoais, incluindo um processo por meio do qual os titulares podem reclamar a precisão das informações.					
Sua estrutura de governança de dados pessoais especifica quando as atualizações são apropriadas com base nas finalidades e tipos de tratamentos de dados pessoais, bem como leva em consideração os interesses do titular.					
Você grava (com meios tecnológicos próprios) quando e onde os principais dados pessoais são coletados, incluindo datas de correções ou atualizações de tais dados.					
Você realiza controles in loco periódicos, avaliações ou auditorias em bancos de dados para garantir que os principais dados pessoais estejam precisos, completos e atualizados.					
Você tem desenvolvido e implementado políticas e práticas de proteção de dados e privacidade, incluindo garantias adequadas para todos os usos de dados pessoais fora do estabelecimento.					
Você informa terceiros com quem os dados pessoais são compartilhados sobre qualquer modificação pertinente ao dado pessoal compartilhado, e implementa políticas e procedimentos apropriados e/ou mecanismos para fazê-lo, tais como cláusulas contratuais e meios tecnológicos.					

Lista de Verificação Para o Princípio VI - Transparência

DECLARAÇÃO	AVALIAÇÃO			EVIDÊNCIAS	PLANO DE AÇÃO
	Atende	Não atende	Atende parcialmente		
Você comunica aos seus *stakeholders* suas políticas e procedimentos relacionados ao seu Programa de Governança de Dados Pessoais.					
Você comunica aos titulares de dados pessoais qual a finalidade da coleta de seus dados e em que situações transfere-os a terceiros.					
Você comunica aos titulares de dados pessoais a quem dentro da sua organização ele pode dirigir perguntas ou queixas relativas ao tratamento de seus dados pessoais.					
Você comunica quem é seu encarregado de dados pessoais.					
Você comunica aos seus stakeholders como eles podem obter acesso ou corrigir seus dados pessoais.					
Você fornece aos titulares de dados uma descrição de quais dados pessoais você espera divulgar para outras organizações e que tipo de organizações elas são.					

Lista de Verificação Para o Princípio VII - Segurança

DECLARAÇÃO	AVALIAÇÃO			EVIDÊNCIAS	PLANO DE AÇÃO
	Atende	Não atende	Atende parcialmente		
Você adota salvaguardas físicas, técnicas e administrativas para proteger informações pessoais contra perda ou roubo, bem como o acesso não autorizado, divulgação, cópia, uso, modificação, deleção e destruição.					
Você escolhe as salvaguardas de segurança que são compatíveis com o tipo de dado pessoal tratado e os meios utilizados para transmiti-lo.					
Você protege todos os dados pessoais, independentemente do tipo e do formato em que é tratado (armazenado, processado ou transmitido).					
Você deixa seus colaboradores cientes da importância de manter a confidencialidade dos dados pessoais.					
Você implementou processos para impedir o acesso não autorizado a dados pessoais durante a eliminação ou destruição dos mesmos.					
Você implementou e aderiu às políticas e práticas de segurança da informação.					
Você estabeleceu uma política de violação da segurança da informação e comprometeu-se a investigar a causa raiz de tais violações ou incidentes.					

Lista de Verificação Para o Princípio VIII - Prevenção

DECLARAÇÃO	AVALIAÇÃO			EVIDÊNCIAS	PLANO DE AÇÃO
	Atende	Não atende	Atende parcialmente		
Você considera as questões de proteção de dados e privacidade como parte do design de produtos e serviços, processos e práticas de negócios na sua organização.					
Você estabelece a proteção de dados e a privacidade como um componente essencial da funcionalidade dos seus sistemas, produtos e serviços.					
Você prevê riscos e eventos invasivos à privacidade antes que eles ocorram e toma medidas para evitar danos aos titulares de dados pessoais.					
Você trata apenas os dados pessoais de que precisa para seus propósitos legítimos e apenas os utiliza para esses fins.					
Você tem mecanismos para que os dados pessoais sejam protegidos automaticamente em qualquer sistema de TI, serviço, produto e/ou prática de sua organização, para que os titulares não precisem tomar nenhuma ação específica para proteger sua privacidade.					
Você adota uma política de "linguagem simples" para que as pessoas entendam facilmente o que estamos fazendo com seus dados pessoais.					
Você oferece padrões de privacidade fortes, opções e controles fáceis de usar e respeita as preferências do usuário titular de dados pessoais.					
Você utiliza apenas operadores de dados que fornecem garantias suficientes de suas medidas técnicas e organizacionais para proteção de dados por design e por default (desde a concepção e por padrão).					
Você, quando controlador conjunto, determina as responsabilidades e respectivos papéis para o tratamento de dados pessoais, em contrato.					
Você avalia a necessidade para conceber, quando apropriado, uma avaliação de impacto de privacidade quando novos tratamentos de dados pessoais ou mudanças ao tratamento existente de dados pessoais são planejados.					

Lista de Verificação Para o Princípio IX - Não Discriminação

DECLARAÇÃO	AVALIAÇÃO			EVIDÊNCIAS	PLANO DE AÇÃO
	Atende	Não atende	Atende parcialmente		
Você não utiliza arquitetura de tratamento de dados, por meio de filtros que estigmatizam, criam estereótipos ou segregam determinadas categorias de titulares, limitando a atuação destes titulares e/ou forçando-os a determinadas condutas.					

Lista de Verificação Para o Princípio X - Responsabilização e Prestação de Contas

DECLARAÇÃO	AVALIAÇÃO			EVIDÊNCIAS	PLANO DE AÇÃO
	Atende	Não atende	Atende parcialmente		
Você revisou suas políticas de privacidade e seu time está convencido de que sua política está completa e fácil de entender.					
Você deixou claro quem na sua organização é responsável pela governança e gestão da privacidade e proteção de dados pessoais.					
Você tem políticas e práticas de privacidade e proteção de dados que se aplicam aos dados pessoais de seus colaboradores, bem como a de seus clientes e fornecedores.					

Sua Política de Privacidade e seu Programa de Governança de Dados Pessoais articulam claramente que você será responsável por todos os dados pessoais que mantém ou manterá em tratamento, incluindo dados pessoais que tenham sido transferidos para um terceiro para tratamento.					
Você orientou sua equipe, por meio da política interna, quanto aos processos e procedimentos ou treinou seu time para fornecer os dados do encarregado de dados aos titulares que solicitarem.					
Você usa cláusulas contratuais consistentes, estabelecendo papéis e responsabilidades, para garantir um nível comparável ao seu de proteção de dados e privacidade de dados pessoais enquanto eles estiverem sob a custódia de um terceiro para tratamento.					
Você verificou se terceiros estão implementando os controles de privacidade e proteção de dados estabelecidos em seus contratos.					
Sua política de privacidade e proteção de dados atende ao “Princípio da Finalidade”.					
Sua política de privacidade e proteção de dados atende ao “Princípio da Adequação”.					
Sua política de privacidade e proteção de dados atende ao “Princípio da Necessidade”.					
Sua política de privacidade e proteção de dados atende ao “Princípio do Livre Acesso”.					
Sua política de privacidade e proteção de dados atende ao “Princípio da Qualidade dos Dados”.					
Sua política de privacidade e proteção de dados atende ao “Princípio da Transparência”.					
Sua política de privacidade e proteção de dados atende ao “Princípio da Segurança”.					
Sua política de privacidade e proteção de dados atende ao “Princípio da Prevenção”.					

Sua política de privacidade e proteção de dados atende ao “Princípio da Não-Discriminação”.					
Sua política de privacidade e proteção de dados atende ao “Princípio da Responsabilização e Prestação de Contas”.					
Você tem uma política de proteção de dados e privacidade para seu time interno.					
Você treinou seu time para conhecimentos, habilidades e atitudes relacionadas à proteção dos dados pessoais e privacidade, informando-os das políticas de privacidade da organização, dos procedimentos e melhores práticas que devem ser adotadas.					
Você tem meios para identificar quais dos seus colaboradores devem receber treinamento e capacitações voltadas à privacidade e proteção de dados, incluindo novos colaboradores e time existente.					
Você desenvolveu documentação para explicar suas políticas e procedimentos de proteção de dados e privacidade para os clientes e demais stakeholders.					
Você desenvolveu informações para explicar aos seus colaboradores as políticas e procedimentos que se aplicam aos seus próprios dados pessoais.					
Você tem registros e meios suficientes para demonstrar a conformidade com suas obrigações em relação ao tratamento de dados pessoais realizado como controlador e/ou operador.					

5 Apêndice A

FAQ Para Efeito do Presente *Framework* Principiológico

O que é **privacidade**?

Privacidade (calcado no inglês *privacy*) é o direito à reserva de informações pessoais e da própria vida pessoal: *the right to be let alone* (literalmente "o direito de ser deixado em paz"), segundo o jurista norte-americano Louis Brandeis, que foi provavelmente o primeiro a formular o conceito de direito à privacidade, juntamente com Samuel Warren em 1890. Brandeis inspirou-se na leitura da obra do filósofo Ralph Waldo Emerson, que propunha a solidão como critério e fonte de liberdade.

Pode ser também entendida como a vontade de controlar a exposição e a disponibilidade de informações acerca de si mesmo, o que é chamado de regulação dos limites: no âmbito da liberdade negativa, ou seja, liberdade que o indivíduo tem de controle sobre a entrada e saída de declarações de si mesmo e a quantidade de contato que se tem com outras pessoas. Esse processo tem implicações diretas no tipo de relação que o indivíduo exerce com e sobre outras pessoas em sua vida.

O que é proteção de dados?

A proteção de dados é o uso justo e adequado de dados sobre as pessoas. Tem relação com o direito fundamental à privacidade - mas, em um nível mais prático, de liberdade positiva. Trata-se de criar confiança entre pessoas e organizações no sentido de que haja respeito a uma liberdade positiva, uma permissão legal, de se utilizar dados pessoais para uma finalidade específica. O que devolve às pessoas o seu direito de ter controle sobre sua própria identidade e suas interações com os outros, permitindo que encontrem um equilíbrio com os interesses mais amplos da sociedade.

A proteção de dados também é essencial para a inovação. As boas práticas de proteção de dados são vitais para garantir a confiança do público, o envolvimento e o suporte a usos inovadores de dados nos setores público e privado.

Quem é o titular de dados pessoais para a LGPD?

É a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Qual o conceito de dados pessoais na LGPD?

Toda informação relacionada à pessoa natural identificada ou identificável.

Qual o conceito de dados pessoais sensíveis na LGPD?

Todo dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Qual o conceito de tratamento de dados pessoais na LGPD?

A LGPD define tratamento de dados pessoais de forma bastante abrangente, partindo da coleta até a eliminação, passando pelo armazenamento e manuseio. Em síntese, a lei traz uma série de operações para conceituar tratamento de dados pessoais:

- toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Quem são os agentes de tratamento de dados previstos na LGPD?

O controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
O operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Qual o conceito de dado anonimizado na LGPD?

É o dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Quem é o encarregado de dados pessoais ou DPO (*Data Protection Officer*)?

É a pessoa (física ou jurídica) indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

O que é pseudonimização de dados?

É o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Qual o conceito de consentimento no âmbito da LGPD?

É a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Qual o conceito de bloqueio de tratamento no âmbito da LGPD?

É a suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

Qual o conceito de eliminação de tratamento no âmbito da LGPD?

É a exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

Qual o conceito de uso compartilhado de dados no âmbito da LGPD?

É a comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

O que é a Autoridade Nacional de Proteção de Dados?

É o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

6 Apêndice B

Bibliografia e Outras Fontes Confiáveis de Consulta

Proteção de Dados Pessoais - A Função e os Limites do Consentimento
por Bruno Ricardo Bioni

Fundamentos De Direito Digital
por Marcel Leonardi

Comentários ao GDPR. Regulamento Geral de Proteção de Dados da União Europeia
por Viviane Nóbrega Maldonado e Renato Opice Blum

LGPD, Lei Geral De Proteção De Dados
por Viviane Nóbrega Maldonado E Renato Opice Blum

Portal da Privacidade
www.portaldaprivacidade.com.br

The Privacy Cast (Podcast sobre Privacidade e Proteção de Dados)
https://www.spreaker.com/show/the-privacy-cast

Site do Dr. Frederico Meinberg - Promotor de Justiça, Coordenador da Unidade Especial de Proteção de Dados e Inteligência Artificial – ESPEC do Ministério Público do Distrito Federal
https://fredmeinberg.com.br/

7 Sobre a Fundacred

Somos uma fundação de direito privado, sem fins lucrativos, que faz gestão de crédito educacional, em parceria com uma rede de mais de 200 instituições de ensino conveniadas em todo o Brasil. Nossa oferta é baseada em um modelo sustentável, que engaja estudantes em um ciclo contínuo e virtuoso de acesso à educação. **O resultado são serviços com o menor custo privado**, tanto para estudantes quanto para instituições de ensino, a menor taxa de inadimplência do Brasil e um crescimento de 331,25% nos últimos 5 anos. Nos orgulhamos de ter colaborado para a transformação sustentável de **mais de 80 mil vidas ao longo dos nossos 47 anos**.

Além do nosso compromisso com o acesso à educação, queremos que a nossa atuação impacte na transformação do mundo. Por isso, adotamos, desde 2016, os **Objetivos do Desenvolvimento Sustentável** (ODS), estabelecidos pela Assembleia Geral das Nações Unidas, e recentemente nos tornamos signatários do Pacto Global da ONU. Nossos valores são pautados e praticados de dentro para fora, o que nos permite, por exemplo, sermos reconhecidos pela certificação do **Great Place to Work** (GPTW).

As soluções de crédito educacional da Fundacred são **CredNEX**, **CredTEC**, **CredIES**, **CredCORP** e **CredNEO**. As ofertas aproximam estudantes e prestadores de serviços educacionais do ensino médio, cursos técnicos, ensino superior (graduação e pós-graduação, inclusive stricto) e cursos livres, bem como empresas que queiram investir em suas equipes.

CredNEX
Crédito educacional para o **ensino médio**

CredTEC
Crédito educacional para o **ensino técnico**

CredIES
Crédito educacional para o **ensino superior**

CredCORP
Crédito educacional **corporativo**

CredNEO
Crédito educacional para **cursos livres**

Por Que Somos Fundamentais?

Mesmo com programas governamentais de incentivo, o acesso à educação ainda não está no patamar que deveria. Em 2016, por exemplo, diversos cortes em bolsas foram realizados e isso acarretou na diminuição de oferta nas universidades, deixando uma parcela significativa de estudantes longe do ensino superior.

Por conta disso, a Fundacred tem se mostrado uma excelente alternativa aos estudantes. Com ela, o acesso à educação é facilitado e sem riscos de falta de investimentos, garantindo que o estudante possa terminar o curso.

Os Benefícios

Conseguimos melhorar nosso trabalho atualizando processos por meio de investimentos em tecnologia. **Dessa forma os estudantes não ficam presos a uma longa burocracia para que consigam efetivar e utilizar seus créditos educacionais**, proporcionando acesso à educação de forma simplificada.

E a IE também tem benefícios. **Com investimentos na melhoria dos processos**, as instituições de ensino garantem menores taxas de evasão de seus estudantes e a restituição é cobrada pela Fundação, garantindo também uma menor taxa de inadimplência.

Nosso Propósito

Transformar vidas, promovendo acesso à educação.

Nossa Declaração da Estratégia

Ser a melhor opção de crédito educacional conectando e multiplicando as oportunidades com **pioneirismo, menor custo privado, sem fins lucrativos e atuando em escala para:**

- **Estudantes** motivados a ascender intelectual, social e economicamente.
- **Prestadores de Serviço Educacional** motivados a captar, recuperar e fidelizar seus estudantes, gerindo seu programa de crédito educacional de modo a ajudá-los a cumprir sua missão, obter resultados e assegurar sua perpetuidade.
- **Organizações** motivadas a desenvolver e fidelizar seu capital humano com segurança jurídica, menor esforço operacional e retorno sobre o investimento.

Nossos Valores

Valor	Decodificação sintética	Decodificação detalhada
PAIXÃO PELO QUE FAZ	O que nos motiva	Somos movidos por profundo sentimento humano em torno de um propósito transformador que nos entusiasma, nos engaja e nos faz dar o melhor de nós todos os dias.
SUCESSO DO CLIENTE	Nossa razão de existir	Estabelecemos relações de parceria, entendendo os desafios e colocando nossa experiência a serviço da busca de soluções para os nossos estudantes, prestadores de serviço educacional e empresas, fazendo do seu sucesso a nossa razão de existir.
DESENVOLVIMENTO SUSTENTÁVEL	Nosso compromisso com o hoje e o amanhã	Agimos de forma sustentável e ética diante de todos os stakeholders, alinhamos nossas prioridades e estratégias com os pilares: social, econômico e ambiental, entendendo que nossas ações de hoje impactam e transformam nosso amanhã e asseguram perpetuidade.
INTEGRIDADE	Nosso jeito de fazer negócios	Pautamos nossas relações na idoneidade, honra e ética, com atitudes de moral plena e incorruptível.
VALORIZAÇÃO DAS PESSOAS	A forma colaborativa com que estabelecemos nossas relações com as pessoas	Pautamos nossas relações internas e externas no respeito, no compartilhamento e no cuidado constante com as pessoas, prezando pelo seu desenvolvimento e geração de ambientes saudáveis.
TRANSFORMAÇÃO	Nossa principal contribuição para um mundo melhor	Acreditamos no poder transformador da educação, na forma com que inclui e promove a evolução da sociedade e do país.

O Futuro

Queremos, com base em nosso trabalho e esforço, transformar mais de um milhão de vidas por meio da educação até 2062. Como pretendemos fazer isso? **Colocando em prática ações que busquem mostrar ao estudante que a educação é o melhor caminho para mudanças significativas.**

Contate-nos:

https://www.fundacred.org.br/site/contato

FUNDACRED

fundacred.org.br

@fundacred