LGPD LEI GERAL DE PROTEÇÃO DE DADOS

Como Implementar a LGPD na Prática

PLANO SI

SUMÁRIO

PLANO SI

INTRODUÇÃO

Da mesma forma que ocorreu com a GDPR na Europa, agora é a vez do Brasil demonstrar maior proteção e transparência na coleta e uso de dados pessoais, sejam eles de clientes, fornecedores, colaboradores ou moradores de um condomínio.

O que mais preocupam as empresas são as sanções que tornam-se riscos independente de vazamentos ou não de dados, bastando a sua “não-conformidade” e adequação, são passíveis de multas que podem variar de 2% de sua receita anual até 50 milhões de Reais.

E você? Está nesse grupo que precisa se adequar às novas regras da LGPD?

Então confira abaixo todos os itens que preparamos para você considerar no momento de implementação!

DEFINIÇÕES

AUTORIDADE NACIONAL: com base no texto da Lei Geral de Proteção de Dados, a Autoridade Nacional de Proteção de Dados (ANPD) é uma entidade que irá ajudar na regulamentação e fiscalização do cumprimento da LGPD.

Esse órgão já era citado no texto original, mas a medida provisória 869/18 foi responsável por caracterizá-lo como uma autoridade pública integrante da Presidência da República.

A medida provisória também detalhou os atributos da ANPD, que se resumem em editar as normas de proteção de dados, monitorar o cumprimento da lei, implementar ferramentas que melhorem a comunicação entre empresas, autoridades e titulares, fazer estudos sobre proteção de dados no exterior e aplicar sanções.

CONTROLADOR: a lei define como controlador a “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” que são coletados.

É importante frisar que o controlador só pode coletar dados caso o titular tenha autorizado ou em algumas situações específicas, conforme a legislação. Também cabe ao controlador manter o sigilo dos dados confiados, e prestar contas às autoridades.

ENCARREGADO: o encarregado é a figura que faz a intermediação entre o controlador, o titular e a ANPD. Também chamado de DPO (Data Protection Officer), essa pessoa física ou jurídica é indicada pelo controlador dos dados.

De acordo com o texto da lei de proteção de dados, as atribuições do encarregado são: aceitar reclamações dos titulares, prestar esclarecimentos e adotar providências; receber comunicações da autoridade nacional e adotar providências; orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais e executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

DADO ANONIMIZADO: é descrito como “dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento”. Em outras palavras, trata-se de uma informação que foi descaracterizada em algum nível para que o seu titular não possa mais ser identificado, mas que ainda é importante para o controlador.

O artigo 12 ainda afirma que os dados anonimizados não são considerados pessoais e a legislação não se aplica a eles, salvo em casos em que o processo de anonimização for revertido e seus titulares novamente identificáveis.

OPERADOR: é a empresa ou profissional diretamente responsável pelo tratamento dos dados. Tanto o operador quanto o controlador devem manter registros sobre o tratamento de dados. A ANPD pode solicitar esses relatórios para verificar se os procedimentos estão em conformidade com a lei.

O controlador e o operador também possuem a responsabilidade sobre o vazamento ou quaisquer tipos de danos causados aos titulares. A seção que trata sobre ressarcimento de danos determina que “o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei”.

PORTABILIDADE DE DADOS: o texto da LGPD não tem um conceito definido para portabilidade de dados, mas podemos considerar que se trata da migração de informações de um controlador para outro.

Por exemplo, caso você tenha contratado um plano de telefonia com uma operadora e deseja migrar para outra, a primeira companhia deve facilitar o processo e enviar suas informações para a nova contratada.

Importante dizer que a portabilidade deve ser solicitada pelo titular e que a antiga controladora não pode reter nenhum tipo de informação.

RELATÓRIO DE IMPACTO: é descrito como uma “documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco”.

Conforme mencionado, tais relatórios devem ser elaborados pelo operador e pelo controlador, pois podem ser solicitados pela ANPD, podendo assim ser suprimidas informações referentes aos segredos industriais e/ou comerciais.

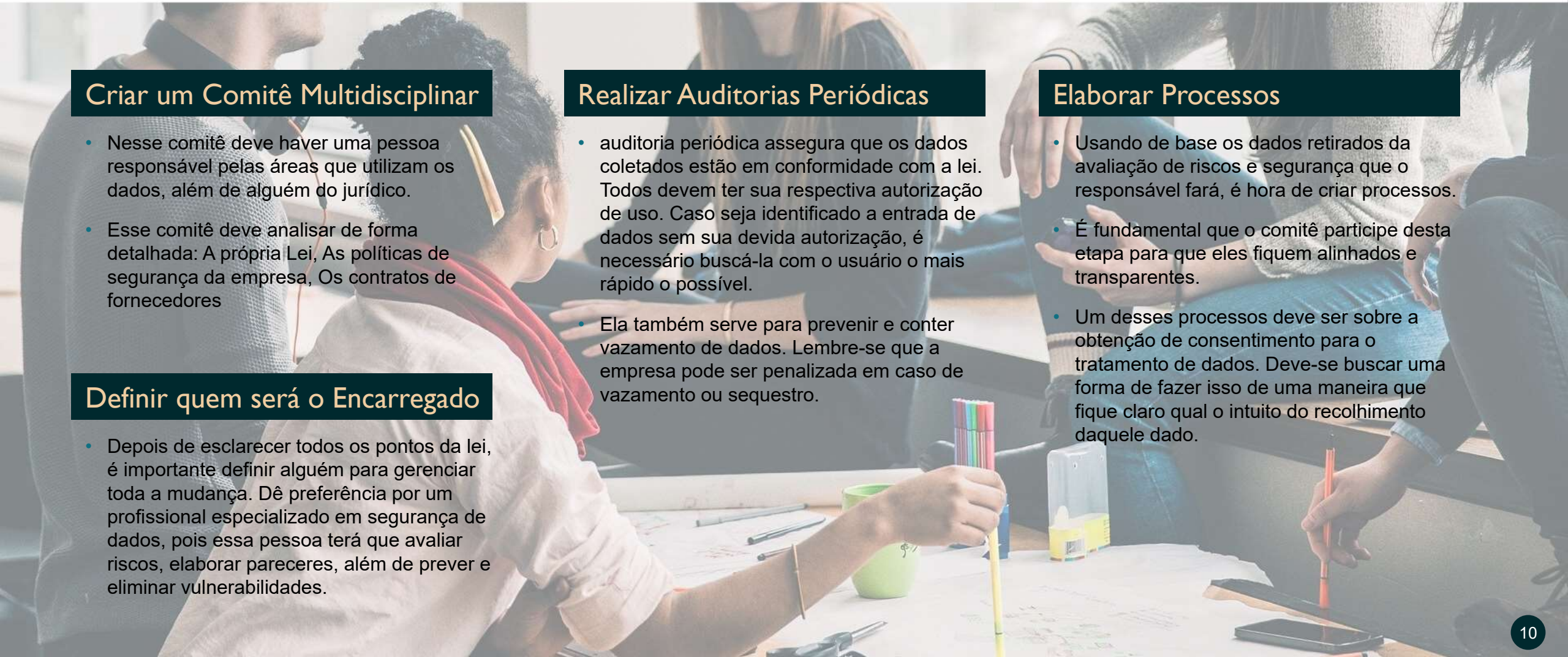
TRATAMENTO DE DADOS: toda operação que utiliza informações pessoais, incluindo a coleta, armazenamento, classificação, reprodução, transmissão e descarte.

USO COMPARTILHADO DE DADOS: é o compartilhamento de informações pessoais por duas ou mais empresas, órgãos ou pessoas, sejam elas do mesmo grupo econômico ou não.

Sendo legal havendo finalidade lícita e o cumprimento de suas competências legais e havendo autorização específica. Caso o compartilhamento de dados sensíveis esteja ligado a vantagens econômicas, poderá ser objeto de vedação e sanções legais. E isso deve valer para entidades públicas e privadas.

O titular possui o direito de saber sobre o compartilhamento de seus dados pessoais que compartilhou e para qual finalidade.

COMO COMEÇAR!



Criar um Comitê Multidisciplinar

- Nesse comitê deve haver uma pessoa responsável pelas áreas que utilizam os dados, além de alguém do jurídico.
- Esse comitê deve analisar de forma detalhada: A própria Lei, As políticas de segurança da empresa, Os contratos de fornecedores

Definir quem será o Encarregado

- Depois de esclarecer todos os pontos da lei, é importante definir alguém para gerenciar toda a mudança. Dê preferência por um profissional especializado em segurança de dados, pois essa pessoa terá que avaliar riscos, elaborar pareceres, além de prever e eliminar vulnerabilidades.

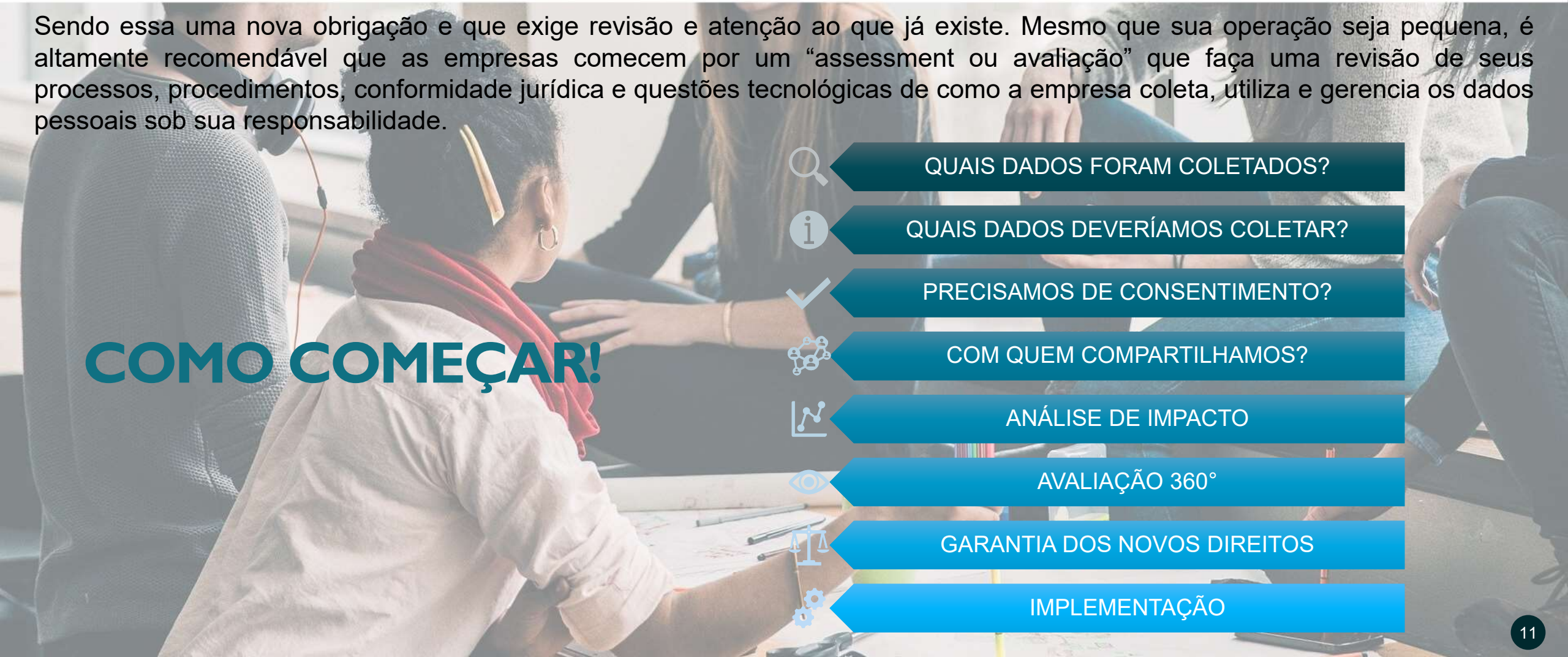
Realizar Auditorias Periódicas

- auditoria periódica assegura que os dados coletados estão em conformidade com a lei. Todos devem ter sua respectiva autorização de uso. Caso seja identificado a entrada de dados sem sua devida autorização, é necessário buscá-la com o usuário o mais rápido o possível.
- Ela também serve para prevenir e conter vazamento de dados. Lembre-se que a empresa pode ser penalizada em caso de vazamento ou sequestro.

Elaborar Processos

- Usando de base os dados retirados da avaliação de riscos e segurança que o responsável fará, é hora de criar processos.
- É fundamental que o comitê participe desta etapa para que eles fiquem alinhados e transparentes.
- Um desses processos deve ser sobre a obtenção de consentimento para o tratamento de dados. Deve-se buscar uma forma de fazer isso de uma maneira que fique claro qual o intuito do recolhimento daquele dado.

Sendo essa uma nova obrigação e que exige revisão e atenção ao que já existe. Mesmo que sua operação seja pequena, é altamente recomendável que as empresas comecem por um “assessment ou avaliação” que faça uma revisão de seus processos, procedimentos, conformidade jurídica e questões tecnológicas de como a empresa coleta, utiliza e gerencia os dados pessoais sob sua responsabilidade.



COMO COMEÇAR!

- QUAIS DADOS FORAM COLETADOS?
- QUAIS DADOS DEVERÍAMOS COLETAR?
- PRECISAMOS DE CONSENTIMENTO?
- COM QUEM COMPARTILHAMOS?
- ANÁLISE DE IMPACTO
- AVALIAÇÃO 360°
- GARANTIA DOS NOVOS DIREITOS
- IMPLEMENTAÇÃO

TRATAMENTO DE DADOS

- Assegurar que todos os dados coletados são realmente necessários para a operação do negócio.
- Minimizar a exposição dos usuários e garantir sua integridade durante a coleta e processamento.
- Utilizar as mais seguras ferramentas para coletar e tratar as informações.
- Mapear em quais momentos da navegação ou da relação jurídica são coletados dados dos usuários.
- Verificar se há a necessidade do compartilhamento ou integração dos dados coletados com terceiros.
- Possui transferência “Internacional” dos dados, e com segurança compatível ao exigido na LGPD/GDPR?

PLANO SI

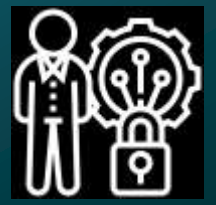
TIPOS DE DADOS RECOLHIDOS

DADOS SENSÍVEIS: Informações que, ao serem compartilhadas, podem gerar desconforto para o usuário, como religião, opinião política e origem étnica.

DADOS PESSOAIS: Identificação direta, como nome, sobrenome ou apelido.

DADOS QUE IDENTIFIQUEM PESSOAS: outros dados como Ids, matrículas internas, números de telefone e e-mails também podem ser considerados como dado pessoal quando permitirem a identificação de um indivíduo.

SEGURANÇA

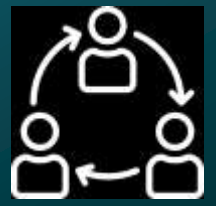


PLANO SI

- Delimitar níveis de acesso para que apenas os usuários que realmente precisam utilizar as informações, possuam acesso a elas.
- Fortalecer a segurança por meio de novas camadas de proteção em hardware e software.
- Considerar as funções e atividades que serão exercidas pelo encarregado de Dados (DPO) para que possa garantir o cumprimento das regras do LGPD e estabelecer boas práticas de processamento na ponte entre a Empresa, Titular dos dados e as Autoridades.
- Aplicar boas práticas de Segurança da Informação e de Governança de acordo com o tamanho da organização.

- Junto com uma assessoria de governança e conformidade, uma assessoria técnica, como também jurídica se fazem necessárias para assegurar o compliance, identificar os riscos e propor formas de lidar com eles.
- Firmar acordos de confidencialidade e sigilo com fornecedores e colaboradores.
- Avaliar a necessidade de compartilhar dados com terceiros.
- Realizar avaliações de impactos à privacidade incluindo o “Data Discovery” e “Health Check” e “assessments” para mapear que dados a organização coleta e como estes são utilizados.

ACESSIBILIDADE E DIREITOS DOS TITULARES



- Criar ou atualizar termos de uso que informem aos clientes sobre a coleta de dados. É preciso informar quais informações estão sendo colhidas, como e a finalidade.
- Garantir que os clientes possam fazer a portabilidade dos dados, caso desejem.
- Criar procedimentos que permitam a remoção dos dados, caso os titulares assim exigirem.

Direitos ao Titular dos Dados

- SABER COMO SEUS DADOS SERÃO USADOS
- POSSUIR ACESSO AOS DADOS PROCESSADOS
- REMOÇÃO DOS DADOS PESSOAIS
- PORTABILIDADE DOS DADOS
- PROMOVER A CORREÇÃO DOS DADOS PESSOAIS
- RESTRINGIR O USO DOS DADOS
- ANONIMIZAÇÃO DOS DADOS
- INFORMAÇÃO SOBRE O COMPARTILHAMENTO COM TERCEIROS

INCIDENTES DE SEGURANÇA

- Criar uma Política de Segurança que tenha um Plano de Comunicação e que notifiquem as autoridades e orientem aos clientes afetados no prazo definido (72 horas na GDPR).

- Capacitar colaboradores para que possam sanar dúvidas e informar aos clientes sobre os vazamentos, correção de informações e exclusão de dados pessoais.

- Acionar o plano de gestão de crises em cenários específicos, com assessoria jurídica.

DPO (DATA PROTECTION OFFICER)

A LGPD também determina a necessidade de um encarregado de dados, o ***Data Protection Officer – DPO*** pelas empresas que realizam a coleta de dados pessoais.

A função do ***DPO*** consiste em atuar como o canal de comunicação a empresa, titulares dos dados pessoais e autoridades governamentais na assistência quanto as práticas de tratamento de dados, bem como, verificar se estas estão em conformidade com a legislação e políticas internas e prestar esclarecimentos.

QUAIS SERÃO AS RESPONSABILIDADES DO DPO?

A LGPD estipula que o ***DPO*** possua conhecimentos aprofundados na legislação e práticas de segurança da informação, proteção de dados pessoais às quais a empresa coleta. Desta forma, as atividades de um ***DPO*** consistem basicamente em:

- **Receber reclamações e comunicações dos titulares dos dados pessoais, prestar esclarecimentos e orientar sobre as providências;**
- **Receber comunicações de órgãos reguladores e adotar as providências cabíveis;**
- **Orientar os colaboradores envolvidos no tratamento e manuseio de dados pessoais dos usuários;**
- **Orientar os colaboradores e prestadores da empresa a respeito das práticas a serem tomadas em relação à proteção de dados pessoais dos usuários;**
- **Manter registros de todas as práticas de tratamento de dados pessoais conduzidas pela empresa, incluindo o propósito de todas as atividades desenvolvidas.**

JURÍDICO

O Relatório de Impacto é um documento que pode ser solicitado pela a ANPD e auditado, para comprovação de quais medidas e forma de condução a proteção de dados pessoais é executada internamente na empresa.

Para que a empresa não sofra sanções é necessário verificar:

- **Se os Termos de uso estão atualizados e em conformidade com termos da LGPD e outras normativas pertinentes.**
- **Se a empresa possui todas as autorizações e anuências expressas dos usuários para todos os serviços que irá prestar (“o consentimento”).**
- **A existência de contratos entre prestadores e empresas terceiras contendo obrigações claras e bem definidas em relação ao acesso, manutenção e exclusão dos dados dos usuários.**
- **Contar com uma assessoria jurídica para assegurar o compliance, identificar os riscos e propor formas de lidar com outros projetos de lei que podem impactar a proteção de dados dos usuários.**

COMO PODEMOS AJUDAR?

A PLANO SI é especializada em temas relacionados ao âmbito da Segurança da Informação, Governança, Conformidade, Riscos e Continuidade de Negócios, além de oferecer amplo apoio e assessoria no Direito Digital e Empresarial, com mais de 22 anos de experiências em apoio aos nossos diversos clientes nacionais e internacionais e dos mais diversos setores da econômicos.

PLANO SI

Necessidades Imediatas

- Palestras, reuniões e treinamentos.
- Validação jurídica de quais dados podem ser coletados, que necessitam de consentimento e o tempo de guarda.

Governança e Conformidade

- Marco Civil da Internet, Lei Geral de Proteção de Dados, Resolução 4.658 Bacen.
- Aplicação de diversos regulamentos para mercados específicos.

Elaboração de Metodologias

- Elaboração conjunta do Relatório de Impacto à Proteção de Dados Pessoais (DPIA) para acesso, exclusão ou modificação de dados pessoais.

Assessoria em Direito Digital

- Revisão das cláusulas e contratos com fornecedores e agentes internos e externos.
- Elaboração / Revisão das Políticas e Termos de Uso.
- Assessoria e apoio jurídico especializado em questões sobre Segurança da Informação, Políticas de Uso e Privacidade.

Encarregado de Dados (DPO)

- Terceirização do DPO ou Encarregado de Dados as a Service.

Gestão de Incidentes

- Atuação preventiva ou reativa em casos de vazamento de dados, fraudes e incidentes.

ENTRE EM CONTATO CONOSCO

planosi.com.br

contato@planosi.com.br

+ 55 (11) 3280-1414