LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

FUNDAÇÃO BENEFICENTE DE PEDREIRA – FUNBEPE

Introdução

Esta Cartilha foi desenvolvida pelo Comitê de Implementação da LGPD da Fundação Beneficente de Pedreira – FUNBEPE e possui caráter informativo, pois consolida um conjunto de informações que objetivam facilitar a compreensão da Lei Geral de Proteção de Dados (LGPD) e seus impactos, orientando os controladores, encarregados e operadores sobre seus respectivos deveres e destacando os direitos dos titulares de dados pessoais que se relacionam com esta instituição.

Privacidade de proteção de dados são assuntos que estão em alta nos últimos anos, isto se da pelo fato de que, cada dia mais uma quantidade enorme de dados pessoais, inclusive dados sensíveis, vem sendo coletados, processados e armazenados por sistemas computacionais. À primeira vista, parece que a LGPD é uma lei complexa. No entanto, devemos entende-la como a lei que regulamenta o uso, a proteção e a transferência de dados pessoais no Brasil. Pensando nisso, essa cartilha foi criada para fornecer um conjunto simples de regras para a segurança, transparência, confidencialidade de dados, privacidade e proteção de informações pessoais na coleta, armazenamento e tratamento dos dados usados nesta instituição.

O que é LGPD?

A Lei 13709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais, é um marco legal que tem por objetivo a privacidade dos indivíduos mediante a criação de um sistema de proteção e garantias dos seus dados pessoais, em documentos físicos ou digitais, os quais precisam ter essa proteção legal.

Quais os dados protegidos pela LGPD?

DADO PESSOAL: Informação relacionada à pessoa natural identificada ou identificável. Essa informação representa todo e qualquer dado que possa tornar uma pessoa identificável, como: nome, CPF, identidade, endereço, telefone e até mesmo dados comportamentais (preferencia de navegação na internet, preferencias de pesquisa em um navegador, o numero identificador e IP;

DADO ANONIMIZADO: Dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

DADO PESSOAL SENSÍVEL: É uma categoria especial de dados pessoais, que ante a possibilidade de ser utilizado para fins discriminatórios, esta sujeito a regras mais rigorosas para o seu tratamento, como por exemplo dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente a saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

QUEM É O CONTROLADOR, O ENCARREGADO E O OPERADOR

Controlador

Pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais.

É o agente de tratamento que tem o dever de tomar todas as decisões acerca do tratamento dos dados pessoais e assegurar que as ações e atividades vinculadas a seu processamento se encontrem em conformidade.

Operador

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador.

É o agente de tratamento de dados que deverá realizar essa atividade segundo as instruções fornecidas pelo hospital.

Encarregado da Proteção de Dados

Pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador, os titulares e a autoridade nacional, suas atribuições estão descritas nos incisos I a IV do § 2º do art. 41 da Lei federal nº 13.709/2018.

Princípios para se tratar os dados pessoais

Princípios do tratamento de dados pessoais(Art. 6º):

1. Finalidade
2. Adequação
3. Necessidade
4. Livre acesso
5. Qualidade dos dados
6. Transparência
7. Segurança
8. Prevenção
9. Não discriminação
10. Responsabilização e Prestação de Contas

LGPD na área da saúde

Todas as áreas que lidam com dados pessoais no exercício de suas atividades precisam se atentar para o tema da proteção de dados pessoais em conformidade com a LGPD. A área da saúde realiza reiteradamente tratamentos de dados sensíveis, o que traz a necessidade de adequação a LGPD de forma ainda mais determinante.

Assim, é inegável a necessidade do setor de saúde, que já dispõe de uma serie de regulamentações e normas setoriais próprias envolvendo o sigilo e confidencialidade das informações dos pacientes e usuários do sistema de saúde, de se atentar para a privacidade e proteção de dados pessoais dos titulares, conforme regramento trazido pela Lei Geral de Proteção de Dados Pessoais.

Atendimento aos pacientes em hospitais, ambulatório e pronto socorro

Hospitais em circunstancias emergenciais ou não, utilizam dados pessoais dos pacientes para identifica-los, bem como para aferir sua situação de saúde por meio da anamnese, procedimento médico em que se verificam os parâmetros vitais relacionados a pressão arterial, temperatura corporal, glicemia, reflexos neurais, nível de consciência e outros condizentes com o contexto clinico, histórico, medicamentoso, entre outras informações.

As informações referentes ao atendimento são registradas no prontuário médico, assim o documento é considerado SIGILOSO, não podendo ser compartilhado com ninguém sem que haja consentimento expresso do paciente.

A unidade hospitalar deverá intensificar as preocupações relacionadas a manutenção da confidencialidade dos documentos do paciente, principalmente seu prontuário médico, garantindo que eles sejam armazenados de forma segura e acessados somente pelos profissionais que de fato precisem ter conhecimento das informações clinicas do paciente.

EXAMES

Nos casos de exames laboratoriais e de imagens os dados pessoais podem ser utilizados para identificação do paciente e dos demais profissionais de saúde envolvidos, para verificação dos exames e procedimentos solicitados pelo médico responsável ou, ainda para melhor diagnóstico e tratamento do paciente.

Nos casos de exame realizados em unidades sem vinculo com o estabelecimento hospitalar, onde o paciente não procura recebe-los para mostra-los ao médico solicitante permanece a responsabilidade de guarda, pois foram produzidos em decorrência de suas atividades especificas, devendo ser observado o definido na resolução CFM nº 1.821/07. O dever de guarda em relação aos exames cessa com a retirada do paciente, podendo ocorrer através de responsável legal e mediante a protocolo de retirada, no entanto, é dever da instituição ficar arquivada uma via do laudo emitido.

Os exames sejam laboratoriais ou de imagens, são considerados dados sigilosos, pois contém informações pessoais sensíveis do paciente, assim a sua divulgação ainda que para fins científicos ou educacionais, sem a autorização expressa do paciente é proibida.

Proteção de dados em sistemas digitais corporativos

Apesar dos benefícios da tecnologia não podemos esquecer que a utilização desta deve ser aliada ao tratamento de dados pessoais de saúde, que podem ser, inclusive, de pessoas em situação de vulnerabilidade, como idosos e crianças.

A tecnologia demanda de cuidados adicionais, de cunho técnico e administrativo, sobre tudo de treinamento dos profissionais, para a garantia da privacidade dos titulares de dados pessoais.

É necessário que a equipe técnica da unidade hospitalar fique atenta para que não haja vazamento de dados através de ataques maliciosos que poderão prejudicar.

Farmácia

A farmácia detém ampla base de dados dos pacientes que se encontram internados na unidade hospitalar, através das prescrições médicas que são enviadas solicitando a separação dos medicamentos, tendo acesso a nome, idade, leito, além de dados clínicos e histórico de medicamentos. Assim é necessário o cuidado para que os dados sensíveis do paciente não sejam divulgados a terceiros não autorizados.

Tratamento de dados de saúde pela unidade hospitalar

Verifica-se que o país está cada vez mais caminhando para a utilização da tecnologia na gestão da saúde, o que se mostra relevante, mas que, por outro lado, demanda maturidade da unidade hospitalar para que se tenha estrutura adequada para garantir a segurança dos dados pessoais.

As empresas de atenção à saúde como hospitais, clínicas, operadoras de saúde, entre outras, devem compartilhar uma série de informações cadastrais e de saúde dos seus pacientes com o Ministério da Saúde, para que esse, na posse de tais dados, possa verificar as necessidades da saúde pública e elaborar políticas públicas capazes de atender a população de forma eficiente.

Além disso, para tornar mais eficaz a utilização de dados na saúde, bem como para diminuir a assimetria de informação nesse ecossistema, foi criada a Rede Nacional de Dados em Saúde, que une todos os registros eletrônicos de saúde em uma mesma base de dados e que está acessível a qualquer profissional ou empresa que tenha necessidade de consultá-la, desde que haja o consentimento do paciente para tanto.

Tratamento de dados de saúde de colaboradores

A unidade hospitalar além dos dados de seus pacientes, deve se preocupar com os dados dos seus colaboradores como médicos, enfermeiros, farmacêuticos, recepcionistas, faxineiros e todos os profissionais que atuam na unidade.

O departamento de Recursos Humanos, possui dados pessoais dos colaboradores que são utilizados para fins de admissão, registro do vínculo empregatício e compartilhamento dos dados com instituições como o Ministério do Trabalho e da Fazenda, em cumprimento a obrigações legais, dados de saúde ocupacional, dados para pagamento, benefícios e dependentes, entre outros.

Importante destacar ainda que é obrigação dos empregadores zelar pela saúde dos seus funcionários e, para tanto, têm responsabilidade legal sobre o controle do ambiente de trabalho, garantindo que seja salubre.

O Departamento de Recursos Humanos realize a coleta dos dados, os quais deverão ser tratados de forma segura e restrita.

Tratamento de dados de crianças e adolescentes

O artigo 14 da LGPD prevê que o tratamento de dados pessoais de crianças e adolescentes deva ser realizado no seu melhor interesse, estabelecendo, contudo, regimes diversos para quando o tratamento se referir a dados desses indivíduos.

O artigo 2º do Estatuto da Criança e Adolescente (Lei nº 8.069/90), considera-se criança o indivíduo com até 12 anos de idade incompletos. A LGPD prevê em seu artigo 14, §1º, que o tratamento deverá, obrigatoriamente, contar com o consentimento de, pelo menos, um dos pais ou do responsável legal.

Essa exigência pode trazer dificuldades práticas, já que, em alguns casos, os estabelecimentos que lidam com dados pessoais de crianças, sobretudo em se tratando de hospitais, estão atuando com situações emergenciais, nas quais não haverá tempo para a coleta prévia do consentimento dos pais. Para ocasiões como essa, a lei traz uma exceção, que permite eventual tratamento de dados pessoais de crianças sem o consentimento exigido. O objetivo é garantir a proteção da vida da criança. Nesse caso, os dados podem ser utilizados uma única vez e sem armazenamento. Mas, sob hipótese alguma, podem ser repassados a terceiros.

Compartilhamento de dados sensíveis

O compartilhamento de dados sensíveis somente é permitido se for verificada alguma das seguintes situações:

- Consentimento do titular;

- Cumprimento de obrigação legal ou regulatória pelo controlador;

- Pela Administração Pública, para a execução de políticas públicas;

- Para a realização de estudos por órgãos de pesquisas com anonimização dos dados sempre que possível e consentimento do titular ou responsável legal;

- Para o exercício regular de direito em contratos e processos judiciais, administrativos ou arbitrais;

- Para a proteção da vida ou incolumidade física do titular ou terceiro;

- Para a tutela da saúde, em procedimento realizado por profissionais da área de saúde, serviços de saúde ou autoridade sanitárias;

As hipóteses para compartilhamento de dados estão dispostas no art. 7º da Lei Geral de Proteção de Dados.

Os direitos que os titulares tem sobre seus dados

O artigo 18 da LGPD determina os direitos do titular sobre seus dados:

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I.- confirmação da existência de tratamento;
II.- acesso aos dados;
III. - correção de dados incompletos, inexatos ou desatualizados;
IV. - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
V. - 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;
VI. - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
VII.- informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
VIII.- informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

Consentimento

O consentimento é uma das possibilidades para que aconteça o tratamento de dados. É uma manifestação livre pela qual o paciente concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Para compartilhamento dos dados, o consentimento tem que ser específico. Deve ser por escrito ou por outro modo que comprove que essa é sua vontade, além de estar destacado em cláusula separada das demais.

Não são aceitas autorizações genéricas para o tratamento dos dados. O consentimento deverá ser para finalidades determinadas e não para "melhoria dos serviços" ou para "melhorar sua experiência", como geralmente as autorizações aparecem.

IMPORTANTE! O consentimento será nulo se tiver sido obtido com base em informações falsas, insuficientes ou que não tenham sido claras.

Consentimento para tratamento de dados pessoais sensíveis

A regra geral é que o tratamento de dados pessoais sensíveis só ocorrerá se tiver seu consentimento, que deverá ser de forma específica e destacada.

Mas, há situações em que o consentimento é dispensado.
São basicamente as mesmas mostradas no tratamento dos demais dados pessoais e também será dispensado quando os dados
forem utilizados para medidas de garantia de prevenção à fraude e de sua segurança nos processos de identificação e
autenticação de cadastro em sistemas eletrônicos.

ATENÇÃO! Ao contrário do que ocorre com o tratamento dos demais dados pessoais, os dados sensíveis não serão utilizados para a execução de contratos ou para atender interesses legítimos do Controlador ou, ainda, para proteção ao crédito SE NÃO TIVER O CONSENTIMENTO do titular!

Importante! Dados referentes à saúde só poderão ser compartilhados nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia, em benefício do interesses do titular e para permitir a portabilidade de dados, quando solicitada pelo titular e para as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de saúde.

- É proibido o compartilhamento de dados pessoais sensíveis referentes à saúde, com objetivo de obter vantagens econômicas.

- As operadoras de planos privados de assistência à saúde não poderão utilizar o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade e na exclusão de beneficiários.

O sigilo médico diante da LGPD

O dever de sigilo médico está previsto no Código de Ética Médica, o qual prevê que o médico deve guardar sigilo a respeito das informações que tenha conhecimento no desempenho de suas funções, exceto no caso de previsões legais.

Com o advento da LGPD, o tratamento de dados sensíveis vinculados à saúde passou a receber proteção garantida por Lei, o que induz à maior atenção e cuidado das informações pessoais inerentes à saúde.

É importante destacar que a LGPD não faz menção específica ao sigilo médico. No entanto, dispõe acerca do dever de tratamento adequado dos dados pessoais sensíveis no que concerne aos dados de saúde, conforme mencionado nesta cartilha.

Sendo assim, as disposições da LGPD reforçam a proteção de dados pessoais de pacientes, bem como objetiva proteger direitos fundamentais, tais como privacidade, liberdade e o respeito à autonomia de escolha do paciente quanto ao acesso de seus dados pessoais sensíveis por outrem, princípios assegurados no sigilo médico estabelecido no código de ética de medicina.

Responsabilidade pelo descumprimento da lei

A LGPD traz uma série de sanções administrativas para o caso de descumprimento de seus preceitos (art. 52):

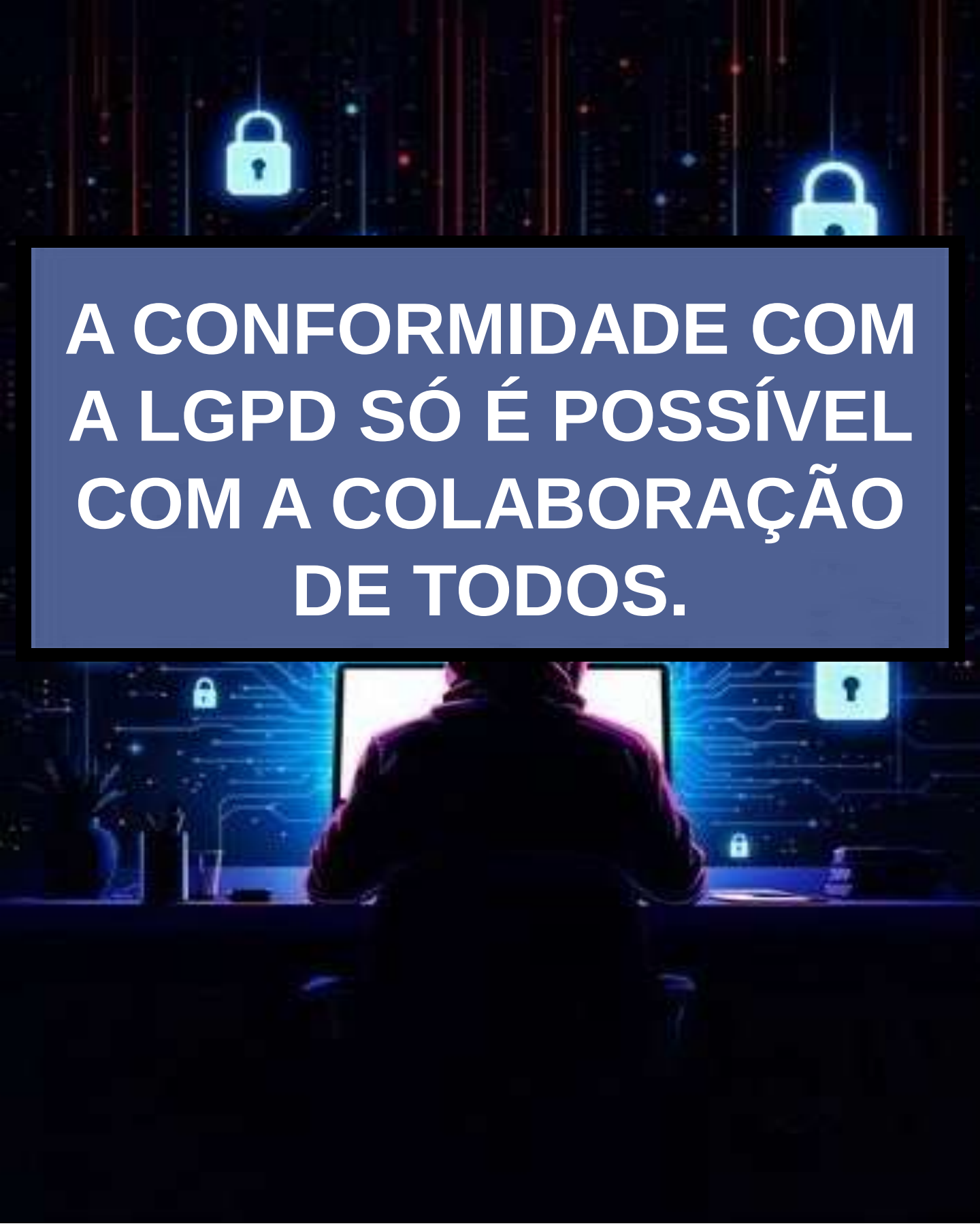
- Advertência com indicação de prazo para adoção de medidas corretivas;
- Multa simples de até 2% limitada a R$ 50 M (cinquenta milhões de reais) do faturamento da pessoa jurídica de direito privado por infração;
- Multa diária;
- Publicização da infração;
- Bloqueio dos dados pessoais a que se refere a infração até sua regularização;
- Eliminação dos dados pessoais a que se refere a infração;
- Suspensão do tratamento dos dados pessoais a que se refere a infração;
- Proibição parcial ou total de exercer atividades de tratamento de dados.

Vale destacar que todas essas sanções são administrativas, ou seja, é possível que haja ainda eventual responsabilização por danos na esfera judicial.
As sanções são aplicadas à empresa, no entanto, o colaborador que descumprir as obrigações previstas na legislação poderá responder administrativa, civil e/ou criminalmente.

Qual é a responsabilidade dos colaboradores?

Todos os processos devem prever a proteção de dados pessoais, sendo que cada colaborador é responsável, em sua respectiva esfera de atribuição, por preservar e proteger os dados pessoais sob sua responsabilidade, estando, para isso, prezando pela ética e boas práticas, assim segue algumas orientações:

- Não fotografe e nem compartilhe fotos de prontuários, diagnósticos, processos e etc. em redes sociais;
- Cuide de seu login e senha. Não compartilhe;
- Não compartilhe dados pessoais se não tiver determinação para isso;
- Banco de dados pessoais requer maior cuidado dos operadores;
- Utilize ferramentas corporativas para tratar dados pessoais;
- Ao proteger os dados pessoais de alguém, você estará cuidando indiretamente da proteção dos seus dados, pois todos nós somos titulares de dados;



A CONFORMIDADE COM A LGPD SÓ É POSSÍVEL COM A COLABORAÇÃO DE TODOS.

AGRADECEMOS A ATENÇÃO!

FUNDAÇÃO BENEFICENTE DE PEDREIRA – FUNBEPE