DECISION
TECNOLOGIA E INOVAÇÃO

LGPD

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS.
SEGURANÇA E CONFIDENCIALIDADE
DA INFORMAÇÃO.

/ PORTAL DO CONHECIMENTO

seu
plano
de carreira
está
ON

A Decision está ligada
no seu futuro.

A Lei Geral de Proteção de Dados Pessoais (n° 13.709/2018) foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo.

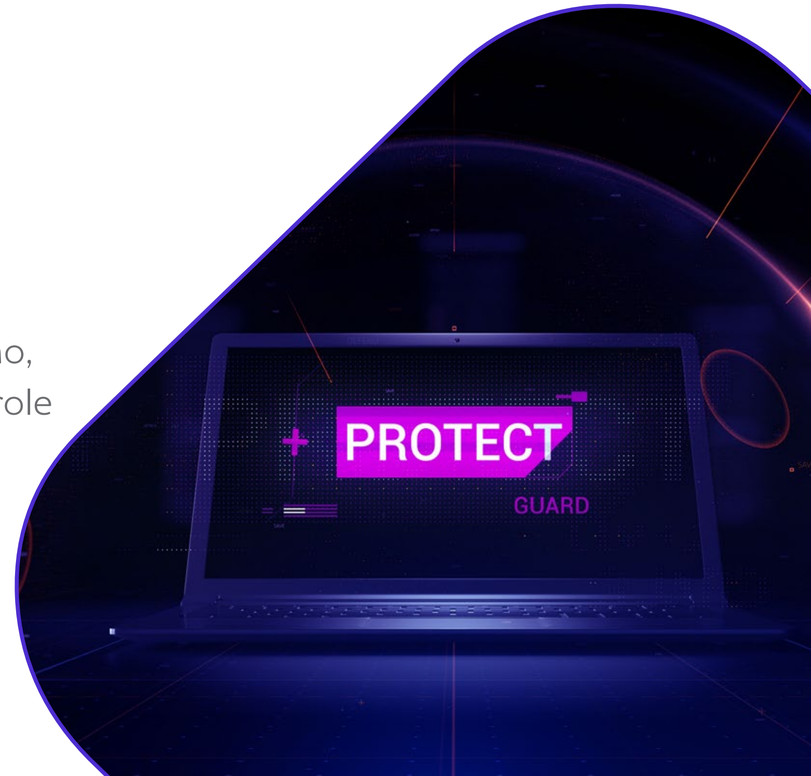
Essa Lei versa sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado e engloba um amplo conjunto de operações efetuadas em meios manuais ou digitais.

LGPD

No âmbito da LGPD, o tratamento dos dados pessoais pode ser realizado por dois “agentes de tratamento”, o Controlador e o Operador:

O Controlador é definido pela Lei como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

O Operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Considera-se “tratamento de dados” qualquer atividade que utilize um dado pessoal na execução da sua operação, como, por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.



O que são dados pessoais

A Decision no uso de suas atribuições legais, necessita manusear dados pessoais para efetivação dos direitos dos colaboradores e clientes, em especial para adequações quanto as legislações trabalhistas e fiscais.

São considerados dados pessoais : O nome completo do colaborador, Número do Registro Geral (RG), Número do Cadastro de Pessoa Física (CPF), dados bancários, número e dados da carteira de trabalho do colaborador e dados de contato como endereço e telefone.
É direito do colaborador que os dados pessoais sejam devidamente armazenados em local próprio e com rigoroso controle e que não possam ser divulgados a terceiros sem o prévio aceite e conhecimento por parte do colaborador.

É importante reforçar que esses documentos são inerentes ao contrato de trabalho conforme pressupõe a legislação, devendo a empresa realizar a devida guarda.

Como manusear dados pessoais?

Ao colaborador conforme contrato de trabalho assinado entre as partes, compete manter as informações pessoais atualizadas, em especial no tocante aos dados de contato e pagamento que são partes inerentes para processamento das obrigações legais.

Sempre utilizar as plataformas da empresa como: site, e-mails e programas oficiais para manusear as informações, eis que as plataformas oficiais são certificadas e seguras para manuseio das informações, bem como, fiscalizadas através de severos protocolos de segurança.

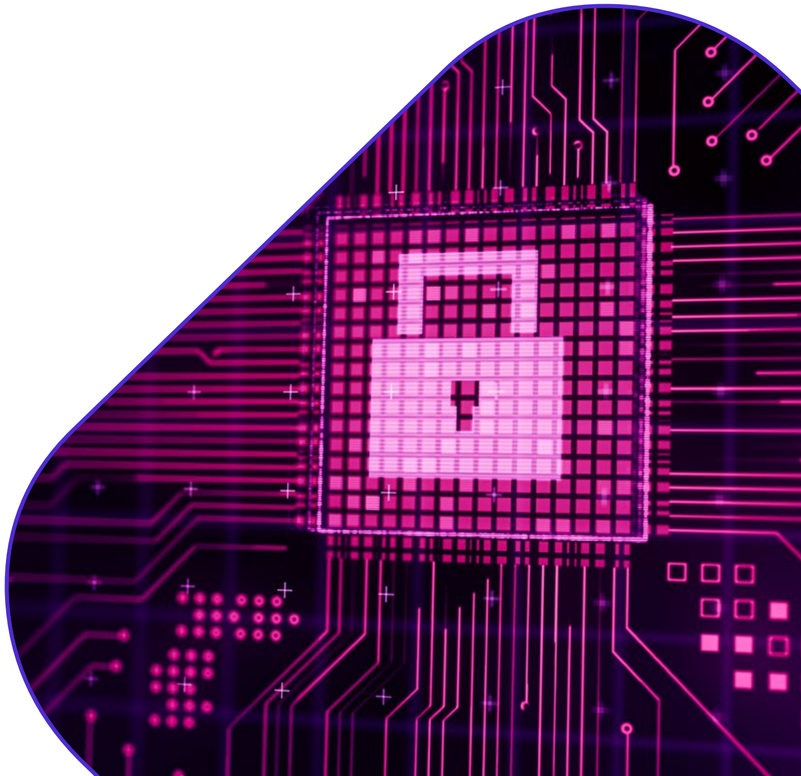
Cabe ao colaborador quando não possível serem utilizadas as ferramentas da empresa, solicitar aprovação e se valer de programas ou sites validados, com programas de antivírus e certificados de segurança. Na dúvida se algum dado pessoal foi manuseado de forma indevida, a Decision deverá ser prontamente notificada para propositura de protocolo de atendimento de exposição indevida de dados.

Confidencialidade da Informação

No ato da contratação todos os colaboradores assinam o termo de confidencialidade, que é a garantia de que o colaborador não usará as informações para beneficio próprio, e ou exposição inadequada, evitando assim a exposição indevida de dados de clientes, da empresa ou de qualquer outro elemento que possa auferir vantagem ou não.

As informações a que por competência da função ou por facilidade de acesso vierem a ser manuseadas pelo colaborador deve limitar-se plenamente ao exercício e limite legal de utilização para a função, jamais sendo compartilhada ou utilizada em meio não compatível com o devido, sendo avaliada cada situação incidindo as sanções disciplinares devidas.

Caso o colaborador identifique qualquer problema na utilização dos dados deverá reportar imediatamente á empresa para abertura de protocolo de segurança.



Segurança da Informação

É o conjunto de medidas para garantir que a confidencialidade, integridade e disponibilidade das informações da organização e do indivíduo seja preservada de forma devida.

A confidencialidade tem a ver com a privacidade dos dados da organização. Esse conceito se relaciona às ações tomadas para assegurar que informações confidenciais e críticas não sejam roubadas dos sistemas organizacionais por meio de cyber ataques, espionagem, entre outras práticas.

Garantindo a confidencialidade dos dados

Dentro da companhia existem mecanismos de controle (como gestão eletrônica de documentos, contrato de confidencialidade, adequação aos sistemas conforme as normas reguladoras, tanto internamente quanto externamente) que garantem pelo grau de severidade da informação tratada qual acesso deve conter cada usuário, garantindo assim, que apenas os usuários que necessitam manusear tenham acesso as informações confidenciais, pelo nível de acesso de cada um, conforme preconiza a LGPD.

Além das políticas internas de tratamento de dados como: mesa-limpa, auditorias de sistemas e ferramentas de controle de exposição de dados confidenciais, matriz de riscos, fluxo de processos com ponto de controle, tanto a empresa quanto clientes possuem departamentos responsáveis pelo monitoramento do tratamento de dados, como departamento de Compliance, Gestão de Riscos além de processos de controle de Departamento Pessoal e Recursos Humanos, voltados a garantir a integridade dos processos e informações.

Práticas para a segurança da informação

Mantenha seu computador atualizado, executando as ações solicitadas e verifique a eficiência como tempo de processamento, capacidade de armazenamento, demora para reiniciar;

Sempre acionar Detectar vulnerabilidades de hardware e software.

Faça sempre **checagem de segurança** em seu antivírus;

Cópia de segurança: manter sempre um back-up das informações em local apropriado com segurança, seja em HD externo, Pen-drive ou na Nuvem, respeitando os protocolos de segurança de cada modalidade.

Firewall: é um mecanismo de controle do tráfego de dados entre os computadores de uma rede interna e destes com outras redes externas. Ele trabalha segundo protocolos de segurança (TCP/IP, IPSec, HTTP etc.) que garantem o correto funcionamento da comunicação entre as duas pontas, visando impedir intrusões.

Assinatura digital: é uma forma de identificação do usuário que está acessando aos recursos de TI, ela dá validade legal aos documentos digitais, assegurando a autenticidade do emissor da informação.

Biometria: o acesso às informações somente é liberado para a pessoa autorizada, levando em consideração as suas características físicas (impressão digital, voz ou padrões da íris do olho ou do rosto inteiro.).

Práticas para a segurança da informação

Seguir a política de confidencialidade e mesa limpa, mantendo documentos guardando em armários ou gavetas que possam ser trancados, respeitar e tipificar os documentos enviados, não deixar documentos impressos parados na impressora ou sobre mesa.

Não utilizar de seu e-mail corporativo para assuntos pessoais;

Não repassar ou acessar indevidamente informações e assuntos corporativos;

Não compartilhar senha e não permitir que nenhum usuário acesse seu equipamento utilizando de suas senhas;

Responder pela guarda e proteção dos recursos computacionais colocados á sua disposição para o trabalho;

Ativar suas senhas de proteção para Correio Eletrônico e Sistema Operacional, sob orientação do Gestor de Liberações da área de TI;

Buscar conhecimento necessário para a correta utilização dos recursos de hardware e software.

Relatar prontamente à área de TI qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus, etc;.

Práticas para a segurança da informação

Comprometer-se em não auxiliar terceiro ou não provocar invasão dos computadores ou da rede de dados, conforme artigo 154-A do Código Penal Brasileiro.

Uma das formas mais avançadas de garantir a segurança da informação é a decisão pela utilização de uma estrutura de computação em nuvem. Essa estrutura tem três categorias distintas: nuvem pública, privada ou híbrida;

Descarte: cuidado com o descarte das mídias e/ou qualquer informação confidencial. Para mídias físicas, garantir que o descarte seja feito em local apropriado;

Garantir que o computador contenha senha de acesso e que sempre esteja bloqueado quando não estiver em uso;

Trocar as senhas de acesso aos sistemas periodicamente;

Garantir a correta utilização do equipamento, utilizando apenas sites autorizados e com certificado de segurança;

Utilize filtros spam nos e-mails para evitar vírus,

Como reportar incidentes de dados?

Sempre que surgirem duvidas sobre a exposição de dados ou manuseamento indevido de dados de qualquer natureza, deverá ser reportado através dos canais oficiais de denúncia:

Através do anonimato pelo site: www.decisionbr.com.br
(botão “DENÚNCIA”)

Através do reporte direto ao RH pelos telefones disponíveis de cada localidade, além do reporte a área de compliance. Toda denúncia é apurada e toda suspeita de desvio de informações ou exposição indevida de dados é realizada com a devida expertise, sendo vedada qualquer retaliação, bem como não há qualquer punição pelo envio da informação, sendo inclusive uma obrigação legal sempre reportar qualquer ato que possa ser suspeito, ou qualquer suspeita de desvio de informações.

Comentários e Declaração de Ciência

Acesse o formulário através do link para a conclusão e ciência desta politica. Caso queira deixamos um espaço para seus comentários, duvidas e sugestões.
Seu feedback é extremamente importante para que possamos aprimorar as politicas, participe!

Agora é hora de fazer a avaliação.

CLIQUE AQUI!

Ou cole e copie o link abaixo no seu navegador!

https://forms.office.com/r/1TUL4sVcf2

Não deixe de realizar os treinamentos:

- Ética
- Ergonomia
- Meio Ambiente

AGOSTO 2021

DECISION
TECNOLOGIA E INOVAÇÃO

/decisionbr.com.br

Matriz São Paulo
Av. Paulista, 1079 – 7º andar – SL 715
São Paulo | CEP 01311-200
T (11) 3297.7449

Unidade Campinas
Av. Barão Itapura, 2294, 13º andar, SL1305
Jardim Guanabara | CEP 13073-300
T (19) 3252.2838