PLAYBOOK A LGPD E OS RHs DAS EMPRESAS.

DIRETIVAS RH

TÓPICOS A SEREM ABORDADOS:

- ✓ **INTRODUÇÃO.**
- ✓ **PRINCIPAIS PONTOS DA LEI 13.709/18.**
- ✓ **RECRUTAMENTO E SELEÇÃO.**
- ✓ **COLABORADORES – CELETISTAS, ESTAGIÁRIOS E MENORES APRENDIZES.**
- ✓ **PRESTADORES DE SERVIÇOS (SERVIÇOS TERCEIRIZADOS).**
- ✓ **CUIDADOS COM CONTRATOS ENVOLVENDO INFORMAÇÕES DE COLABORADORES DO BANCO DE DADOS DA CONTRATANTE QUE VENHAM SER DISPONIBILIZADOS A TERCEIROS.**
- ✓ **FLUXO DE INFORMAÇÕES COM RELAÇÃO A RECURSOS HUMANOS.**
- ✓ **FLUXO DE INFORMAÇÕES EM PODER DE TERCEIROS.**
- ✓ **CUIDADOS A SEREM TOMADOS NA ELABORAÇÃO DE CONTRATOS:**
  - **COM COLABORADORES**
  - **COM PRESTADORES PESSOA JURÍDICA**
  - **COM EMPRESAS PARCEIRAS, EM ESPECIAL: BANCOS, SEGURADORAS, PLANOS DE BENEFÍCIOS, SINDICATOS, CONTABILIDADE EXTERNA, JURÍDICO EXTERNO, DENTRE OUTRAS.**
- ✓ **CUIDADOS NA DEMISSÃO.**
- ✓ **MODELOS DE ADEQUAÇÕES TECNOLÓGICAS**
- ✓ **SOBRE CONSENTIMENTOS.**
- ✓ **LGPD E AS EMPRESAS.**
- ✓ **CONCLUSÃO / CONTATOS**

1. INTRODUÇÃO:

A área de Recursos Humanos se apresenta em uma posição extremamente importante e ao mesmo tempo vulnerável, perante a Lei Geral de Proteção de Dados - LGPD, face ao conjunto de informações que detém, desde um simples currículo que recebe.

Desta forma, deve assegurar por meio de processos e procedimentos, o fiel cumprimento da Lei Geral de Proteção de Dados (LGPD), na busca de garantir a proteção absoluta das informações.

Para tanto, com apoio da alta gerencia, deve disseminar orientações interdepartamentais, bem como, trabalhar ao lado da área de Tecnologia da Informação, de forma a privilegiar e ter como ponto de partida a revisão sistêmica e dos processos e procedimentos internos, que levem ao pleno atendimento da lei quanto à garantia da segurança das informações, de forma que as informações estejam protegidas a ataques de hacker e/ou a compartilhamento não permitido, assegurando assim que a organização esteja em conformidade com o atendimento da legislação, e isenta de penalidades.

2. PRINCIPAIS PONTOS DA LEI:

Após mais de oito anos de debates foi sancionada, em 14 de agosto de 2018, a Lei Geral de Proteção de Dados – LGPD, Lei 13.709/18.

Com a promulgação da Lei Geral de Proteção de Dados – LGPD, tornou-se evidente a urgência quanto a atenção das empresas na revisão dos procedimentos relacionados à coleta, tratamento e armazenamento de dados pessoais, de forma generalizada.

A LGPD tem aplicação a qualquer pessoa, seja natural ou jurídica de direito público ou privado que realize o tratamento de dados pessoais, online e/ou off-line. Assim, podemos afirmar que a Lei possui aplicação ampla e abrangente, que abarca grande parte de projetos e atividades do cotidiano empresarial.

A LGPD dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, estabelecendo regras e limites para empresas a respeito da coleta, armazenamento, tratamento e compartilhamento de dados.

Em linhas gerais, os Titulares dos dados deverão ter total controle sobre todo o processamento de seus dados pessoais, refletindo desta forma, diversas obrigações para os Controladores (a quem competem as decisões sobre o tratamento dos dados) e Operadores (aqueles que tratam os dados de acordo com o estipulado pelos controladores).

A Lei apresenta relevantes princípios para nortear o tratamento de dados pessoais, como:

- Finalidade: Devem atender propósitos legítimos, específicos e devidamente cientificados a seus titulares;
- Adequação: Devem ser compatíveis e com sua funcionalidade;
- Necessidade: Devem ser proporcionais a atendimento de sua finalidade;
- Livre Acesso: Devem permitir consulta facilitada aos titulares, e garantia da integralidade das informações;
- Qualidade: Devem privilegiar dados exatos claros e atualizados;
- Transparência: Que sejam facilmente acessíveis;
- Segurança: Devem apresentar medidas técnicas e administrativas que levem a proteger os dados pessoais de tentativas de invasões e/ou acessos não autorizados, independentemente de terem o caráter acidental ou ilícito.

Os titulares de dados pessoais passam a ter os seguintes direitos:

- Confirmação da existência de tratamento;
- Acesso fácil e a qualquer tempo a seus dados pessoais;
- Poder contar com a correção de dados incompletos, inexatos ou desatualizados;
- Anonimização ou Pseudonimização de seus dados pessoais

- Manifestar o interesse pela Portabilidade de seus dados pessoais;
- Ser atendido quanto a eliminação ou exclusão de seus dados pessoais;
- Ser Informado caso haja o compartilhamento de seus dados pessoais;
- Possibilidade de expressar seu não consentimento quanto a guarda e/ou compartilhamento de seus dados pessoais, ressaltando de que o consentimento é temporal, e desta forma, poderá ser revogado a qualquer tempo.

Tudo isso leva a necessidade das Empresas em adotar medidas de segurança, governança e boas práticas;

Para tanto, deverão contar com uma figura intitulada de Encarregado (profissional responsável internamente por orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais, bem como, por orientar e avaliar o cumprimento da Lei);

CONCEITOS RELEVANTES

O QUE SÃO DADOS PESSOAIS?

Dado Pessoal (art. 5º, I): segundo a Lei, dado pessoal é toda e qualquer informação relacionada à pessoa natural identificada ou identificável. Assim, a LGPD traz um conceito amplo e aberto, pois qualquer dado, que isoladamente (dado pessoal direto) ou agregado a outro (dado pessoal indireto) possa permitir a identificação de uma pessoa natural, pode ser considerado como dado pessoal. Exemplos: dados cadastrais, telefones, data de nascimento, profissão, dados de GPS, identificadores eletrônicos, nacionalidade, gostos, interesses e hábitos de consumo, entre outros.

Dado Pessoal Sensível (Art. 5º, II): A Lei é implacável ao tratar dos dados pessoais sensíveis, os quais versem sobre:

- Origem racial ou étnica;
- Convicção religiosa; ou 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.

Dados sensíveis são aqueles dados relacionados a determinada pessoa natural identificada ou identificável por meio dos quais pode sofrer discriminação e, por tal motivo, devem ser considerados e tratados como dados sensíveis.

COMO TORNAR DADOS IMPESSOAIS?

Na busca de não expor as informações tidas como Dado Pessoal Sensível (Art.5º, II) de forma a evitar-se a invasão da privacidade destas informações, a alternativa que a empresa poderá se socorrer, pois se apresenta de forma adequada, é anonimização ou pseudoanonimização da informação, desta forma é possível salvaguardar o titular, pois os dados não permanecem identificáveis.

O QUE A LEI CONSIDERA COMO TRATAMENTO DE DADOS?

Tratamento (art. 5º, X): toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Para se tratar dados pessoais, o que inclui a prática da coleta e todas as demais citadas pelo dispositivo legal como a recepção, classificação, arquivamento e transferência, sempre é necessário ter um fundamento legal.

Nesse ponto, mostra-se importante observar que o CONSENTIMENTO se torna uma das melhores hipóteses legais para o tratamento de dados.

TERMOS RELEVANTES

TITULAR (art. 5º, V): pessoa natural a quem se referem os dados pessoais objeto de tratamento.

CONTROLADOR (art. 5º,VI): pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais.

OPERADOR (art.5º, VII): pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

AGENTES DE TRATAMENTO (art. 5º, IX): o controlador e o operador.
Pela MP n° 869/18 o encarregado, também conhecido como Data Protection Officer ("**DPO**"), não precisa mais ser uma pessoa natural, abrindo espaço, desta forma, para a possibilidade de indicação de pessoas jurídicas, comitês, ou grupos de trabalho, que podem exercer tais funções. Ainda, deixa clara a possibilidade de terceirização de tal serviço.

3. RECRUTAMENTO E SELEÇÃO:

A partir do momento que a empresa abre uma vaga, já deve estar atenta ao cumprimento da Lei Geral de Proteção de Dados, pois, ao receber os candidatos ou seus currículos, independentemente de ser na forma presencial, eletrônica ou meios digitais, passa a se responsabilizar pelas informações coletadas. Deve garantir e assegurar, por meio de processos e procedimentos, a proteção destas informações de forma que iniba seu vazamento, através de um incidente ou compartilhamento não autorizado, cabendo ainda disseminar estes procedimentos a todos os departamentos com objetivo do estabelecimento de cultura interna, quanto a privilegiar-se a proteção das informações de modo amplo dentro da organização.

Deve ainda estar preparada para promover a transparência na busca das informações bem como, de forma clara, esclarecer a finalidade da coleta de cada um dos dados, vindo a colher as concordâncias/autorizações individuais, expressas e firmadas por seu titular, inclusive quanto à manutenção destas informações em seu Banco de Dados.

Caso não haja autorização expressa, tão logo se encerre o processo seletivo, caberá à empresa excluir de seu banco de dados às informações daqueles candidatos não aprovados, levando a empresa manter em

seu Banco de Currículos, somente aqueles candidatos que expressamente manifestaram autorização para tanto.

O QUE FAZER?

a) Incluir TERMO DE CONSENTIMENTO quando do recebimento do Currículo, seja de forma fisica ou eletrônica.
b) Digitalizar TODOS os currículos e descartar (destruir) os currículos físicos.
c) Pseudonimizar os dados dos Titulares no banco de dados de currículos eletrônicos, ou seja, alterar os dados de cadastro para dados fictícios e indexados, por exemplo:
    a. CPF – Alterar para um número indexado
    b. Nome – utilizar apenas o primeiro nome do candidato
    c. Dados de contato – retirar do documento de busca ou criptografa-los.
    d. Desta maneira, os currículos poderão ser analisados e separados por qualquer pessoa sem que se permita a violação da confidencialidade.
    e. Os currículos destacados para contato deverão ser encaminhados à pessoa específica que detém o controle do arquivo original indexado e que fará os devidos contatos e agendamentos.
    f. Se o Banco de Currículos for compartilhado com outras empresas, o Titular deverá dar o Consentimento Explícito para tal e deverá haver um "Termo de Compromisso de Utilização de Informações" com a empresa destinatária dos dados.

4. ADMINISTRAÇÃO

Casos não previstos e/ou exceções deverão ser tratados entre a área solicitante e a área de Recursos Humanos e, por fim, submetidos à aprovação da Diretoria.

5. COLABORADORES (CELETISTAS, ESTAGIÁRIOS, MENORES APRENDIZES...):

Este item implica em duas vertentes, a primeira de Colaboradores já existentes e outra de Futuros Colaboradores.

a) **Colaboradores já Existentes**:

Os colaboradores já existentes necessitarão ter seus cadastros atualizados, de forma a assinar um Termo de Consentimento autorizando a utilização destes dados pela empresa, cabendo à empresa destacar as razões que a levam necessitar das informações, públicas ou privadas, dando ampla ciência ao titular para onde e de que forma seus dados pessoais serão mantidos e qual finalidade serão utilizados.

Nos termos da lei é recomendado que a empresa opte em manter em seu Banco de Dados, somente aquelas informações imprescindíveis ao desenvolvimento das atividades laborais. Neste ponto tratando-se de colaboradores existentes, se faz necessário no momento da higienização das informações, identificar os dados disponíveis no cadastro que possam ser descartados, de forma a identificar aqueles dados e/ou informações que devem ser mantidos, colhendo a concordância e autorização da permanência junto ao titular.

É salutar e se faz necessário a alteração dos termos do Contrato de Trabalho, de forma a inserir em sua redação cláusulas que atendam aos requisitos da LGPD.

b) **Novos Colaboradores**:

Dar sequencia nas tratativas iniciadas quando da fase de Recrutamento e Seleção, complementando com a adoção de novo modelo de Contrato de Trabalho, onde o novo colaborador de o conhecimento e manifeste sua concordância quanto à necessidade das informações serem mantidas no Banco de Dados do empregador (exemplos: atender os preceitos da lei do e-social, legislação trabalhista e previdenciária, medicina, higiene e segurança do trabalho...).

c) **Estagiários**:

Com referencia a absorção deste tipo de mão de obra, deve-se ter os mesmos cuidados tidos junto a seus colaboradores, desta feita porem, com relação a que o estagiário manifeste sua ciência e concordância com que suas informações permaneçam no Banco de Dados da empresa, através do Contrato de Estágio, estendendo e compartilhando a responsabilidade junto à entidade Educacional quanto ao cuidado com as informações geradas.

Em todas as situações anteriormente enumeradas, deverá ser redobrada a atenção quanto às informações relacionadas à saúde e outras informações que possam ser entendidas como: preconceituosas, difamatórias, desonrosas ou outra forma que possa significar prejuízo moral.
Outro cuidado deverá ser observado quando tratamos de adolescentes, pois, neste caso as permissões devem ser concedidas por um dos pais ou tutores legais.

O QUE FAZER?

a) Incluir o "Termo de Consentimento" em TODOS os contratos com colaboradores, indicando quais as informações serão arquivadas e a finalidade específica de cada uma delas.
b) Pseudonimizar os dados de acesso público.
c) Manter acesso estritamente restrito ao Banco de dados, inclusive com controle de usuário, senha e log de acessos por usuário.
d) Manter no Banco de dados apenas, e tão somente, as informações absolutamente necessárias e obrigatórias.

6. PRESTADORES DE SERVIÇOS (SERVIÇOS TERCEIRIZADOS):

No caso de serviços terceirizados, caberá à empresa contratante exigir da empresa Prestadora de Serviço (Contratada), documento que manifeste estar cumprindo a risca a LGPD e ao mesmo tempo isente a tomadora de qualquer tipo de responsabilidade. Recomendamos que a tomadora por sua vez evite manter em seu banco de dados informações dos trabalhadores da prestadora de serviços (Contratada).
Recomendamos que as empresas Contratantes exijam uma cláusula adicional, nos seguintes termos:
Exemplo: Clausula "X" – Neste ato, assume que cumpre fielmente de forma segura e sigilosa a Lei Geral de Proteção de Dados – LGPD, respondendo por todos os atos praticados por si ou terceiros que tenham acesso a seu Cadastro ou Banco de Dados, isentando a **CONTRATANTE** de todos e quaisquer tipo de penalidade que venha dar causa.

O QUE FAZER?

a) Contrato com Cláusula especifica de proteção de dados, com as empresas fornecedoras de mão de obra.

b) Não armazenar nenhum dado do colaborador terceirizado que não seja estritamente necessário.

7. CUIDADOS COM CONTRATOS ENVOLVENDO INFORMAÇÕES DO BANCO DE DADOS DA CONTRATANTE QUE VENHAM SER DISPONIBILIZADOS A TERCEIROS:

Neste ponto vale destacar o cuidado em prever-se no Contrato de Prestação de Serviços executado por terceiros (alguns tipos abaixo indicados), para os quais a Contratante disponibiliza informações cadastrais envolvendo: Seu Quadro de Pessoal, Prestadores de Serviços, Clientes e Fornecedores, de forma a responsabilizar estes terceiros quanto à correta e adequada utilização e guarda destas informações, em especial voltadas somente para os trabalhos para os quais foram contratados.

Alguns exemplos destes prestadores:

- Contabilidade Terceirizada;
- Sistema de Folha de Pagamento;
- PPRA – PCMSO
- Bancos (Contas Salário);
- Empresa de Benefícios (Vale Transporte, Refeição, Alimentação)
- Convenio Médico e Odontológico;
- Seguro de Vida e/ou Acidente;
- Entidades de Classe (patronal ou laboral)
- Empresas que venham efetuar campanhas internas de venda aos colaboradores.

O QUE FAZER?

a) Contrato com Cláusula especifica de confidencialidade e de proteção dos dados que estão sendo recebidos pelas Contratadas, destinadas à execução dos trabalhos.
b) Restringir as informações de forma a ser transmitidas aquelas estritamente necessários à execução dos trabalhos.
c) Dados sensíveis deverão ter tratamento diferenciado.

8. FLUXO DE INFORMAÇÕES COM RELAÇÃO A RECURSOS HUMANOS

O Fluxo de Admissão inicia-se na fase de Recrutamento e Seleção, que se desenvolve da seguinte forma.

As informações cadastrais do candidato são geradas às empresa de forma presencial ou eletrônica. Em ambas circunstancias estas informações figuram no Banco de Dados e o cuidado, neste particular, é de que o candidato manifeste seu aceite e/ou aprovação para que seus dados permaneçam em um banco de dados de currículos, isso para o caso de não ser aprovado naquele momento, levando-se em conta de que potencialmente poderá ser aproveitado em outra oportunidade próxima ou não.

Caso o candidato não concorde que seus dados permaneçam em poder da empresa, concluído o processo seletivo suas informações devem ser descartadas imediatamente.

Mesmo que o candidato concorde e autorize a manutenção de seus dados cadastrais, para fortalecer a proteção dos dados, a recomendação é para que estas informações permaneçam no Banco de Currículo de forma Anonimizadas ou Pseudonimizadas.

Na sequencia, a partir do momento em que o processo seletivo é concluído, a área de Recursos Humanos deve providenciar a contratação do novo colaborador, neste caso, para cumprimento da LGPD, faz-se necessário que a área de Recursos Humanos, acrescente aos termos do Contrato de Trabalho, e demais documentos que compõem o processo de admissão, a razão e motivo que justifique para os quais são necessárias determinadas informações cadastrais, colhendo a concordância do titular da informação.

Das justificativas mais relevantes, dentre outras, encontramos a Legislação do e-Social, Legislação Trabalhista e Previdenciária, Receita Federal, Medicina e Segurança do Trabalho.

9. FLUXO DE INFORMAÇÕES EM PODER DE TERCEIROS.

Em todos os Contratos de Prestação de Serviços a Terceiros, cujos principais enumeramos anteriormente (item 5), deverá ser acrescentada uma cláusula de que a empresa Prestadora de Serviço assuma categoricamente que cumpre fielmente a Lei Geral de Proteção de Dados – LGPD, e que isente a Contratante de todos e quaisquer tipos de penalidade na ausência de tal cumprimento.

Principais informações a destacar nas referidas clausulas:

a. Contabilidade Terceirizada: Informações Cadastrais Pessoais e Financeiras da Contratante e de Terceiros;
b. Sistema de Folha de Pagamento: Informações Cadastrais Pessoais e Financeiras;
c. PPRA – PCMSO: Informações Cadastrais, em especial relacionadas à Saúde Ocupacional e Acidentes;
d. Bancos: Informações Cadastrais Pessoais e Financeiras;
e. Empresa de Benefícios (Vales: Transporte, Refeição, Alimentação ou Cesta Básica): Informações Cadastrais Pessoais e Financeiras;
f. Convenio Médico e Odontológico: Informações Cadastrais Pessoais, Financeiras e de Saúde;
g. Seguro de Vida e/ou Acidente: Informações Cadastrais e Saúde.
h. Entidades de Classe (Patronal ou Laboral): Informações Cadastrais Pessoais;
i. Empresas parceiras, as quais efetuam campanhas internas de comercialização de produtos aos colaboradores.

10. CUIDADOS NA ELABORAÇÃO DE CONTRATOS:

CONTRATO DE TRABALHO

Não nos sentimos confortáveis e ao mesmo tempo não identificamos a necessidade de transcrever na integra um determinado modelo de Contrato de Trabalho, visto que as empresas já possuem este instrumento contratual, e o vem utilizando há tempo, assim sendo, cabe-nos ressaltar a necessidade de que a empresa venha acrescentar ao Contrato usual, uma clausula que atenda a LGPD, na qual justifique a necessidade das informações pessoais solicitadas, bem como, a manutenção destas informações em seu Banco de Dados, de forma que o colaborador se declare ciente e autorize o uso e armazenamento em seu Banco de Dados.

Clausula "X" – O Empregador cientifica neste ato ao Empregado de que todas as informações pessoais indicadas neste instrumento foram solicitadas em cumprimento a Lei Geral de Proteção de Dados, LGPD LEI 13.709/18, as quais serão utilizadas no atendimento dos requisitos do Decreto nº 8.373 de 11/12/2014, que trata do Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas – (e-

Social), bem como, da Legislação Tributária emanada dos órgãos da Receita Federal e ,que passado o tempo estabelecido para guarda das informações, estas serão descartadas dos sistemas de controles e banco de dados.

Ciência e autorização do Empregado:_____

Assinatura

Nota: Recomendamos que o Empregador colha do Empregado, autorização especifica e isolada nesta cláusula, independentemente da Assinatura ao final dos termos contratuais.

CONTRATO DE PRESTAÇÃO DE SERVIÇOS – PESSOA JURÍDICA

Como grande parte das empresas, em especial as menores sentirem certa dificuldade na elaboração de Contrato de Prestação de Serviços, envolvendo Pessoa Jurídica, especialmente frente as mudanças das leis trabalhistas, indicamos uma minuta que pode auxilia-las.

COM EMPRESAS PARCEIRAS: (Bancos, seguradoras, Plano saúde, sindicatos, contabilidade externa, jurídico externo)

Neste caso, como os Contratos normalmente são padrões das empresas Prestadoras de Serviços, recomendamos que as empresas Contratantes exijam uma cláusula adicional, nos seguintes termos:

Clausula "X" – Neste ato a CONTRATADA assume que cumpre fielmente de forma segura e sigilosa a Lei Geral de Proteção de Dados – LGPD 13.709/18, respondendo por todos os atos praticados por si, através de colaboradores, prepostos ou terceiros que tenham acesso a seu Cadastro ou Banco de Dados, isentando a **CONTRATANTE** de todos e quaisquer tipos de responsabilidade, assumindo para si as penalidade que venha dar causa.

11. CUIDADOS NA DEMISSÃO:

Acrescentar no Aviso de Dispensa, cláusula que trate da LGPD, a título de sugestão deixamos o transcrito abaixo:

Clausula "X" – Cientificamos neste ato, de que todas as informações pessoais indicadas neste instrumento, foram solicitadas em cumprimento a Lei Geral de Proteção de Dados - LGPD LEI 13.709/18, as quais foram e serão utilizadas no atendimento dos requisitos do Decreto nº 8.373 de 11/12/2014, que trata do Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas – (e-Social), bem como, da Legislação Tributária emanada dos órgãos da Receita Federal, e que passado o tempo estabelecido para guarda das informações, estas serão descartadas dos sistema de controles e Banco de Dados.
É imprescindível que TODAS as informações não obrigatórias de guarda, sejam eliminadas do banco de dados imediatamente após a demissão, salvo a autorização, em contrário e formal, do Titular.

12. MODELOS DE ADEQUAÇÕES TECNOLÓGICAS

A LGPD vai, inegavelmente, unir ainda mais as áreas de Recursos Humanos (RH) e Tecnologia da Informação (TI). Por isso, é importante reforçar que as empresas serão obrigadas a elaborar ou revisar suas políticas internas, definindo de forma bastante clara os setores que poderão ter acesso a dados de candidatos, empregados e terceiros, bem como a forma de utilização de tais informações.

A aplicação de ferramentas adequadas, com interface de fácil implementação, será um dos desafios para fornecedores do segmento da segurança da informação, uma vez que funcionários utilizarão dados providos pela organização, e sua responsabilidade sobre eles será primordial para as políticas da empresa.

Por exemplo: em processos como recrutamento e seleção, será importante que os líderes de TI e RH reestruturem as políticas e os acordos de confidencialidade. Será preciso ter à mão, desde a primeira entrevista, termos de consentimento de uso de dados, que devem ser assinados pelos candidatos. Esse processo deverá deixar muito transparente como a empresa usará esses dados e quais serão mantidos em arquivo.

Abaixo alguns pontos que devem ser analisados para a correta implementação das rotinas internas das empresas.

FLUXO IMPLANTAÇÃO

- Avaliação do cenário atual
- Necessidades de aderência e requisitos do negócio.
- Compliance normativa e regulatória e Analise de GAP.
- Definição de terceirizar ou contratar um DPO (Data Protection Officer).
- Formação de Comitê Multidisciplinar.
- Elaboração de Plano de Ação e de trabalho.
- Elaboração de plano de Administração de Crises.
- Gestão de mudanças.
- Gestão dos Projetos para implementação e entrega.
- Relatórios de Status.

FLUXO OPERACIONAL

- Auditoria sobre os tratamentos de dados existentes.
- Higienização dos Dados e manutenção dos atributos.
- Implementação de rotinas de segurança e acesso ao Bando de dados.
- Gestão de Consentimentos e Anonimizações.
- Plano de Comunicação e Respostas a incidentes de segurança.
- Plano de Análise de Impactos/Riscos.
- Gestão de demandas do Titular – Transparência e livre acesso.
- Gestão do Ciclo de vida dos Dados.
- Certificado de Conformidade a ser seguido por todos os colaboradores e demais que tenham acesso as dados dentro da empresa.
- Definição do DPO.

13. SOBRE CONSENTIMENTOS.

Tirando algumas situações previstas na LGPD, é o TITULAR que define se seus dados pessoais podem ou não ser tratados por terceiros.

Se eleger a principal palavra da Lei Geral de Proteção de Dados Pessoais (LGPD), a escolhida seria, sem dúvidas, **CONSENTIMENTO**.

É o TITULAR, ou seja, a pessoa a quem se referem os dados, que deve de livre e espontânea vontade, ao ser questionado, de forma explícita e inequívoca, autorizar que suas informações sejam usadas, por empresas e órgãos públicos, na hora da oferta de produtos e serviços, gratuitos ou não.

Portanto, com a nova lei, fica claro de que quem utiliza não é o verdadeiro dono do dado, nem tão pouco aquele que o salvaguarda em bancos de dados. O dado pessoal é estritamente da pessoa a quem ele diz respeito. Na teoria isso parece algo óbvio, mas na prática atualmente o entendimento não é bem este, e assim sendo, de forma equivocada, muito dado particular/pessoal esta sendo usado para fins que seu Titular sequer sabe. Uso este, inclusive, que podem até mesmo vir a prejudicá-los.

O Consentimento na prática

Imagine que o Titular autorizou que seus dados fossem utilizados por uma empresa, isso para uso em uma determinada ocasião ou assunto, caso esta mesma empresa necessite utiliza-los para outros fins, a empresa deverá solicitar nova permissão para uso especifico e para esta nova finalidade ou mesmo se pretender compartilhar os dados com outras organizações.

Com isso queremos dar ênfase de que o consentimento deve ser para finalidades determinadas. Isso significa que o consentimento obtido de uma forma muito genérica, sem especificações, serão considerados nulos perante a lei.

Vale lembrar que o Titular pode revogar, a qualquer momento, um consentimento concedido anteriormente e caso a organização altere informações no decorrer do tratamento dos dados o Titular deve ser avisado sobre isso, e neste caso poderá vir a revogar o consentimento, caso não concorde com a alteração.

Quando tratar dados pessoais for condição para fornecimento de produto ou serviço ou para exercício de um direito, o Titular deve ser avisado sobre isso e sobre os meios pelos quais pode exercer seus direitos. E se as informações fornecidas tiverem conteúdo enganoso ou abusivo, ou ainda não forem apresentadas previamente com transparência e clareza, o consentimento será considerado nulo.

Além disso, quando forem feitas mudanças, na finalidade de um tratamento, não compatíveis com o consentimento original, o gestor dos dados deverá informar isso previamente, e dar a opção de revogar o consentimento, se o Titular discordar das alterações propostas. A oposição deverá ser feita mediante manifestação expressa, por meio de procedimento gratuito e facilitado.

Entendemos que para obter-se o CONSENTIMENTO é necessária uma "Moeda de troca" palatável.

Em alguns casos esta "Moeda de troca" é inerente ao negócio, pois haverá a inteira disposição do Titular em não questioná-la. Por exemplo, a inclusão de seus dados em um banco de currículos que poderá gerar futuros frutos positivos. Portanto é necessário um "Data mapping" permanente para que estes dados não sejam utilizados de forma incorreta ou que sejam "vazados".

Uma alternativa para minimizar os riscos é a "**Pseudonimização**" dos dados, ou seja, retirar, dos registros, os dados pessoais que remetam a identificação do Titular. Desta maneira as informações poderão ser manipuladas sem o risco da disseminação e reeditadas quando da necessidade.

14. LGPD E AS EMPRESAS:

Alguns pontos que devem ser analisados com muita atenção antecipadamente:

COMEÇAR AGORA: Um grande erro é pensar que há muito tempo para a entrada em vigor da lei ou que o prazo será estendido. Essa é a desculpa mais comum das empresas que ainda não fizeram nada em relação à lei. O mais alarmante é que elas simplesmente não sabem o que precisam fazer e qual será o impacto em seu negócio e em sua operação.

ACHAR QUE A LEI NÃO SE APLICARÁ AO SEU NEGÓCIO OU “NÃO PEGARÁ”: Até este momento, se seguirmos a lei, ela não faz distinção, por isso as empresas precisam se preparar, lembrando que a inobservância da lei gerará receita ao governo e especialistas do direito, e isso pode trazer prejuízos à saúde financeira.

COMEÇAR O TRABALHO SOZINHO: Não será possível a adequação sem que se crie uma equipe multidisciplinar, a qual deve contar com o estrito apoio da alta administração. Para tanto, inicialmente a empresa deverá juntar todos os interessados, áreas de TI/SI, RH, Risco, Compliance, Governança e Jurídica, formando um comitê multidisciplinar para avaliar as necessidades de adequações internas.

USO DE CONSULTORIA EXTERNA ESPECIALIZADA**:** Como as necessidades que forem identificadas deverão acarretar a mudanças de forma generalizada nas diferentes áreas, uma alternativa viável é se socorrer de consultoria externa especializada.

NOVOS CENÁRIOS: Tudo mudará, já que o proprietário dos dados deverá sinalizar seu consentimento de forma clara e a pessoa jurídica que mesmo assim ignorarem esta prerrogativa estará sujeita a multas de enorme monta, que pode prejudicar sobremaneira a saúde financeira da empresa.

A nova lei prevê em seu teor nove hipóteses que tornam legais os tratamentos de dados. Dentre eles, dois merecem destaque:

É necessário obter o CONSENTIMENTO EXPLÍCITO por parte do titular dos dados. Ele deverá ser claramente informado dos termos de uso e extensão da autorização e precisa concedê-lo livremente.

A partir de agosto de 2020, uma empresa só poderá recolher determinados dados a partir da autorização do proprietário desses dados, ou seja, o titular deverá comprovar que a sua coleta é útil e necessária.

Os titulares dos dados poderão a qualquer momento retificar, cancelar ou até mesmo solicitar sua exclusão.

A LGPD empodera o titular, dando a ele controle sobre seus dados e a possibilidade de punir os responsáveis por qualquer dano causado pelo mau uso de suas informações.

Criada a partir da MP 869/18, a ANPD - Autoridade Nacional de Proteção de Dados é o órgão responsável pela fiscalização da proteção de dados por parte das pessoas jurídicas. A ANPD poderá solicitar, a qualquer tempo, relatórios de riscos de privacidade, às empresas, para certificar-se de que as organizações estão tratando o tema internamente respeitando as condições estabelecidas pela LGPD.

O primeiro passo recomendado para a empresa quanto a adequação, passa pela criação, de um Comitê de Segurança da Informação, a quem caberá analisar a atual situação dos procedimentos internos quanto ao recebimento e guarda das informações recebidas.

Dentro deste processo é importante fazer um mapeamento bem detalhado a respeito de como os dados pessoais são coletados, armazenados e tratados, desde o período de candidatura a emprego, durante e depois de findo o vinculo empregatício, quem teve acesso e se foram compartilhados com terceiros dentro e fora do Brasil.

A partir do resultado dessa análise, será possível avaliar o nível de maturidade dos processos dentro da organização os riscos envolvidos.

Detectadas as deficiências, chega a hora de iniciar os procedimentos para tornar a transação de dados totalmente segura tanto para a empresa quanto para os titulares.

São quatro os atores que fazem parte ativamente da proteção dos dados em cada empresa:

- O **TITULAR** - É o proprietário dos dados, no caso as pessoas físicas,

- **CONTROLADOR** - É representado pelo tomador dos dados, ou seja, as pessoas jurídicas,
- O **OPERADOR** - A empresa responsável pela coleta de dados e sua efetiva segurança através de soluções automatizadas,
- O **ENCARREGADO** - É o profissional que responde pela proteção dos dados da empresa. É o seu representante, que fará contato com a ANPD quando necessário e pode até ser responsabilizado junto com a pessoa jurídica no caso uso inadequado dos dados ou seu vazamento por qualquer motivo.

15. CONCLUSÃO / CONTATOS

O que se conclui diante de todo esse cenário é que a LGPD significa um grande desafio para as empresas, que precisarão rever vários processos de governança e privacidade de dados, tais como:

- Gestão de consentimento (tanto as autorizações quanto as revogações),
- Gestão das petições abertas por titulares dos dados (que em muitos casos deve ser respondida imediatamente),
- Gestão do ciclo de vida dos dados dentro da empresa (data mapping e data discovery)
- Implementação de técnicas de anonimização (os dados nesta condição não serão considerados dados pessoais pela lei, desde que o processo seja comprovadamente irreversível),
- Revisão de todos os CONTRATOS sejam com colaboradores, fornecedores, parceiros e clientes.
- Mapeamento e analise de risco de todas as atividades com dados pessoais, Implementação de Politica de Segurança, Termo de Conduta, Politica de Atendimento ao Titular, Politica de Privacidade ente outros,
- Documentar todo o processo de adequação à LGPD.

A Adequação LGPD é trabalhosa, porém totalmente viável de ser implementada.

A **LGPD** não é uma opção... é uma **OBRIGAÇÃO**

Para implementar um processo que seja **100% legitimado** perante a Lei e que dê embasamento a qualquer processo trabalhista e/ou civil, é necessário o envolvimento pleno de todos os colaboradores que, em algum momento, tenham acesso a dados pessoais.

Nosso produto **LGPD4me** – ***Metodologia Avançada de Auto Adequação LGPD*** - www.lgpd4me.net – foi desenvolvido para que as empresas, de qualquer porte ou segmento, possam implementar os processos e procedimentos com *facilidade*, *agilidade* e a um *baixo custo*.

Uma metodologia já consagrada e aprovada por centenas de empresas que concluíram seus processos **LGPD** em **total conformidade** com as exigências da Lei.

CONTATO:

UMBERTO FORTI
CEO PROGRAMA LGPD 13.709
(11) 4485-0215 (voz e WhatsApp)
contato@lgpd13709.com.br
www.lgpd4me.net
www.lgpd13709.com
www.cursolgpd.com.br
www.ouvidorialgpd.com.br