BREVES PONTUAÇÕES DA LGPD - LEI GERAL DE PROTEÇÃO DE DADOS

BREVES PONTUAÇÕES DA LGPD - LEI GERAL DE PROTEÇÃO DE DADOS

1) DISPOSITIVOS LEGAIS QUE EMBASAM A LGPD

Quer ficar atualizado, busque a legislação e normatização no site do planalto, mais atualizada, impossível. E, pra ficar mais fácil segue o link da nossa lei do momento: **http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.**

Estamos a tratar da LGPD ou Lei Geral de Proteção de Dados Pessoais, que foi sancionada em 27/12/2018, e, se observarmos os destaques da transcrição feita pelo link anterior, há referência a outros dispositivos legais (destaque nosso). Vamos lá:

> **Art. 65. Esta Lei entra em vigor:** (Redação dada pela Lei nº 13.853, de 2019)
> I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e (Incluído pela Lei nº 13.853, de 2019)
> I-A – dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54; (Incluído pela Lei nº 14.010, de 2020)
> ~~II – 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos.~~ ~~(Incluído pela Lei nº 13.853, de 2019)~~
> II - em 3 de maio de 2021, quanto aos demais artigos. (Redação dada pela Medida Provisória nº 959, de 2020)

http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm

LEI Nº 13.853, DE 8 DE JULHO DE 2019 : Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.

http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv959.htm

MEDIDA PROVISÓRIA Nº 959, DE 29 DE ABRIL DE 2020: Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, **e prorroga a** vacatio legis **da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais - LGPD.**

http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Lei/L14010.htm

E, como nada é tranquilo nesse período de pandemia, eis que, o Projeto de Lei 1179/2020 se tornou a Lei 14010/2020 na data de 12/06/2020, e, dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado no período da pandemia do Covid-19.

Importante salientar que toda novidade gera desconfiança, pânico, desespero, protestos, descontentamento, dentre outros adjetivos, mais, a União Europeia possui uma lei similar desde 1995 e sua eficácia é exemplar.

A nossa LGPD irá possuir um órgão fiscalizador, previsto na própria lei, nomeado de ANPD – Autoridade Nacional de Proteção de Dados, a qual ficará encarregada de fiscalizar, orientar, corrigir e penalizar as irregularidades e não adequações da lei em relação ao tratamento de dados pelas empresas.

Resumindo:

A LGPD entrará em vigor, conforme a atual situação, em 03/05/2021, em decorrência da eficácia e aplicação da MP 959/20, que entrou em vigor na data de 03/05/2020. Outrossim, é importante acompanhar o andar desta Medida Provisória, tendo em vista que ela pode não ser convertida em Lei, e, caducar, o que muda a data de vigência da LGPD.

Independentemente da entrada em vigor da LGPD, se em agosto de 2020 ou em maio de 2021, as sanções previstas nela somente serão aplicadas a partir de 01/08/2021, decorrente da Lei 14010/2020 publicada em 12/06/2020, advinda do Projeto de Lei 1179/2020.

Essa alteração de vigência da lei para 2021 entrou em pleitos políticos e empresariais no final do segundo semestre de 2019, se potencializando com a ocorrência da pandemia, sob argumento de que as empresas não estariam prontas, e com dificuldades de se adequarem.

Outrossim, a LGPD foi sancionada em agosto de 2018, e, por possuir certa complexidade, ser de relevante importância e, ainda, gerar impacto em várias vértices, sua *vacatio legis*, ou seja, tempo de adaptação, seria de 02 anos. Mais, como sempre deixamos para última hora, e quase sempre temos prorrogação, o brasileiro não se adequa dentro do prazo proporcionado.

2) OBJETIVO DA LGPD E CONCEITOS

O **objetivo formal da LGPD** é “proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”.

Muito se ouvirá: tratamento de dados.

Tratamento de dados nada mais é do que: coleta; produção; recepção; classificação; utilização; acesso; reprodução; transmissão; distribuição; processamento; arquivamento; armazenamento; eliminação; avaliação ou controle da informação; modificação; comunicação; transparência; difusão ou extração de dados.

A LGPD estabelece regras para coletar, tratar, armazenar e descartar dados.

Dados pessoais: em regra é a qualificação da pessoa (número constante nos documentos como habilitação veicular, registro civil, cadastro de pessoa física, nome, data e local de nascimento, estado civil, profissão, etc), mais ainda, gênero, telefone, endereço residencial, localização via GPS, prontuário de saúde, cartão bancário, renda, histórico de pagamentos, hábitos de consumo, preferências de lazer, endereço de IP dos aparelhos, enfim, tudo aquilo que remeta a identificar a pessoa.

É importante relevar que a LGPD não está taxando o que seriam os dados pessoais, então, pode ser qualquer fato, característica, informação, enfim, o conceito anterior é exemplificativo e não taxativos.

Não obstante a isso, importantíssimo distinguir o que são dados sensíveis e comuns ou não sensíveis, pois isso importará muito no entendimento da adequação e aplicação da LGPD.

Dados sensíveis (artigo 5º, II, LGPD):

- Origem racial ou étnica
- Opiniões políticas
- Crenças religiosas ou filosóficas
- Associação a sindicatos
- Dados genéticos
- Dados biométricos apenas para fins de identificação pessoal
- Dados relativos ao estado de saúde ou à vida sexual e/ou orientação sexual de uma pessoa.

Dados Anonimizados (anônimos): dado relativo a titular que não permite ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Esses dados estão fora da proteção da LGPD.

Dados Pseudo-Anonimizados: processo semelhante ao da anonimização, em que 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. O pseudo-anonimato é incentivado pelo próprio regulamento como forma de reduzir os riscos. Sendo assim, é abrangido pelo LGDP. Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Dados não sensíveis ou comuns é todo e qualquer item que identifique, porém, não esteja elencado na identificação dos dados sensíveis.

DPO ou também chamado de **Data Protection Officer**, ou seja, 'será o cara', este profissional será o guardião do tratamento dos dados na empresa, sendo que pela LGPD não precisa ter certificação, mais toda empresa que precise tratar dados necessita ter este profissional. Este importante indivíduo trabalhará internamente, não poderá acumular funções na empresa sendo apenas e tão somente a ponte entre o titular de dados, a empresa e a ANPD, deverá ser um bom gestor, e ainda, saber gerir dados, deve possuir inteligência e controle emocional, e ter comunicação fluida, simples, direta e subsidiada. Deve ter ética, ser conhecido da empresa para poder gerir melhor o tratamento de dados. E, se ainda possuir conhecimento em Tecnologia da Informação – TI e Jurídico, poderá ainda se destacar e crescer dentro deste novo nicho de trabalho.

Esta figura está prevista no artigo 18 da LGPD.

Resumindo: o DPO será uma espécie de SAC – serviço de atendimento ao cliente, pois ele receberá a reclamação, a dúvida, a sugestão, a solicitação e, dará segmento com sua equipe para adequar, corrigir, ou seja, tratar aquele dado. E será o DPO que irá tratar das situações da empresa – cliente – ANPD.

Ainda, o DPO pode ser um consultor e possuir vários clientes, coordenando mediante auditoria, plano de ação, implementação, fiscalização e comunicação com as partes envolvidas, relevando-se a ética em não atender empresas do mesmo ramo para não incidir uma concorrência desleal.

A LGPD permite, ainda:

a) acesso e retificação dos dados: todo e qualquer cliente deverá ter acesso às suas informações e ao tratamento dado a elas sempre que precisar, e, sem qualquer custos.

b) portabilidade: o cliente poderá pedir a transferência dos seus dados para outra empresa.

c) eliminação: o cliente poderá pedir a eliminação dos seus dados daquela base e empresa, exceto dos órgãos de proteção ao crédito e que estejam ligados aos dados sensíveis de ordem pública.

d) anonimização dos dados: em caso de pesquisas internas ou de marketing, poderá ser solicitada pelo fornecedor dos dados que se mantenha no anonimato.

e) consentimento (opt in)/ revogação (opt out): o fornecedor dos dados pode consentir e depois revogar e vice-versa.

3) PARTES DA LGPD

- **TITULAR DOS DADOS:** é a pessoa física a quem se referem os dados pessoais.
- **AGENTES DE TRATAMENTO:** é a pessoa física ou jurídica, de direito público ou privado, que coleta os dados pessoais e toma as decisões em relação a forma do tratamento, OU, a pessoa que realiza o tratamento de dados pessoais em nome do controlador.
- **ENCARREGADO:** é a pessoa física, indicada pelo controlador, que atua como canal de comunicação entre as partes (controlador, os titulares e a autoridade nacional).

4) PRINCÍPIOS DA LGPD

O artigo 6º da LGPD dispõe dez princípios que devem nortear o tratamento de dados pessoais. São eles:

a) Finalidade: todo tratamento de dados deve ter uma finalidade específica, não é uma questão apenas de ter os dados, é preciso estar estabelecido o motivo.

b) Necessidade: obter apenas os dados necessários, nada mais do que se precise para atingir a finalidade da coleta.

Ressaltando dois pontos:

- Dark data – dados inúteis não devem ser coletados/obtidos.
- Time (tempo) da coleta – para aquele momento, precisa saber a finalidade da demora em usar os dados coletados por exemplo.

c) Transparência: palavra de ordem. Precisa ser especificado quando solicitado o dado, o motivo para qual será usado, quando será usado, por quem será usado, onde, por quanto tempo e por quem será armazenado.

d) Qualidade dos dados: banco de dados deve estar sempre atualizado, utilizando-se das outras ferramentas, princípios e bases para adequar este tratamento de dados.

e) Não discriminação: o tratamento de dados não poderá selecionar, discriminar, priorizar ou criminalizar o fornecedor de dados por religião, antecedentes, nacionalidade, status financeiro, cor, e demais adjetivos pejorativos.

f) Segurança e Prevenção: no tratamento de dados deverá ser aplicado, impreterivelmente, formas de segurança e prevenção, através de técnicas na proteção de dados, para prevenir incidentes de segurança, com o fim de minimizar os danos causados.

g) Adequação: aplicar o meio mais adequado e eficaz para tratamento dos dados daquele seguimento.

h) Livre Acesso: quem cede o dado para algum fim, poderá e deverá ter controle dos dados tanto quanto quem está armazenando e tratando estes dados, pois deve ter livre acesso aos dados. Poderá pedir para quem coletou os dados informações sobre como está sendo tratado aquele dado e deverá ter resposta imediata, sem qualquer ônus. Quem atende esta situação é o DPO.

i) Prestação de contas: todo tratamento de dados deve ser documentado, qualquer ato, seja de implementação, adequação, correção, prevenção, etc, isso porque necessariamente a **ANPD poderá solicitar relatório de impacto à proteção de dados pessoais.**

5) BASES LEGAIS DA LGPD

É tudo aquilo que a lei conferiu à você para justificar o tratamento de dados pessoais, ou seja, tudo o que você faz.

Deve se enquadrar em uma dessas hipóteses (bases legais), que autoriza, legitima o tratamento de dados.

Importante destacar que LGPD não é somente consentimento, mais é uma das bases necessárias para adequação no tratamento de dados. Vejamos:

a) CONSENTIMENTO: A LGPD exige que o consentimento seja fornecido por escrito ou por outro meio que demonstre a manifestação inequívoca de vontade do titular. Quando o consentimento se der por escrito, ele deverá constar em uma cláusula destacada das demais contratuais, que não pode ser genérica, justamente para que seja comprovado que aquele consentimento foi dado para uma finalidade específica de tratamento. Ao coletar dados através do consentimento dos titulares desses dados, será necessário dispor de algum tipo de plataforma que permita a exclusão dos dados após a requisição do titular e que mantenha evidência dessa exclusão para fins de comprovação posterior, caso necessário, tudo de forma gratuita. Portanto, recomenda-se que a coleta de dados se dê com base no consentimento somente de forma residual, caso não seja possível o tratamento de dados através de alguma outra das outras 9 bases legais dispostas na LGPD.

b) OBRIGAÇÃO LEGAL: No caso de uma obrigação decorrente de lei acarretar em um tratamento de dados pessoais por parte de uma empresa, essa estará autorizada a trata-los de modo a cumprir a dita exigência legal ou regulatória. Por exemplo: anotações em carteira profissional de trabalho.

c) PROCESSO JUDICIAL/EXERCÍCIO REGULAR DO DIREITO: Esta base serve para garantir o direito de produção de provas de uma parte contra a outra em um processo judicial, administrativo ou arbitral, pois caso contrário seria cercear o direito de defesa da outra em um processo e infringir os preceitos constitucionais da ampla defesa e do contraditório. Pois, quem daria consentimento para ser processado?

Entretanto, devemos observar quem irá manipular estes dados.

d) EXECUÇÃO DE CONTRATO: o tratamento de dados se dará a pedido do titular dos dados para garantir a execução de um contrato ou de seus procedimentos preliminares. Essa hipótese se assemelha um pouco com o tratamento de dados via

consentimento, com a diferença de que o titular dos dados não poderá revogar o seu fornecimento a qualquer momento, uma vez que a outra parte estará resguardada pela LGPD para poder manter os dados fornecidos pelo titular enquanto durar a vigência do contrato. Um exemplo seria a contratação por parte de um titular de dados de um serviço cujo objeto principal é o tratamento de dados pessoais, tal como acontece com a inserção de dados em um serviço de armazenamento em nuvem.

e) PESQUISA: Aqui é possível o tratamento de dados pessoais feito para realização de estudos por órgãos de pesquisa, e, sempre que possível, estes dados deverão ser anonimizados, a fim de garantir a privacidade dos titulares e evitar possíveis vazamentos, ou seja, não é possível identificar o seu titular, considerando a utilização de técnicas razoáveis na ocasião do tratamento.

f) POLÍTICAS PÚBLICAS: O inciso III do art. 7º da LGPD dispõe que órgãos da administração pública precisam se adequar e cumprir a lei ao tratarem e compartilharem dados pessoais para execução de políticas públicas ou respaldadas em contratos, convênios ou instrumentos congêneres, sem a necessidade de consentimento dos titulares. A Administração Pública somente não estará obrigada a cumprir com as exigências da LGPD no caso de tratamento de dados feito exclusivamente para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação ou de repressão de infrações penais. Similar situação aos serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público.

Uma grande diferença da aplicação da LGPD aos órgãos públicos para o âmbito privado diz respeito às penalidades aplicadas. Para a Administração Pública, não há a previsão de sanção pecuniária, mas apenas a advertência, bloqueio ou eliminação dos dados pessoais a que se refere a infração, sem prejuízo das sanções previstas no Estatuto do Servidor Público Federal, na lei de Improbidade Administrativa e na lei de acesso à informação.

g) PROTEÇÃO DA VIDA: Aqui o tratamento de dados é feito com o intuito de proteger a vida ou a incolumidade física do titular dos dados ou de terceiros. Esta base legal é um autorizador legal cujo objetivo é garantir a proteção de bens de elevado interesse público, tais como a vida e a incolumidade física, desde que devidamente comprovada essa necessidade e exposta a finalidade do tratamento dos dados nesta situação. Inclusive abrange a possibilidade de tratar dados pessoais

sensíveis sem o fornecimento de consentimento do titular, caso sejam indispensáveis para a proteção da vida ou da incolumidade física do titular ou de terceiro, haja vista o interesse público envolvido neste tipo de tratamento.

h) TUTELA DA SAÚDE: Aqui a LGPD também autoriza o tratamento de dados para a tutela da saúde, desde que realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária. Ou seja, é similar à base do item anterior. Provavelmente será um dos itens de maior debate ao longo da formação e consolidação da consciência de proteção de dados na sociedade brasileira.

Entretanto, aqui devemos nos atentar que a LGPD possui lacunas que será ou pelo menos deverá ser suprida pela ANPD – Autoridade Nacional da Proteção de Dados, sim, porque a LGPD não nos conceitua quem serão os profissionais da saúde, nesse caso, devemos usar de outros dispositivos legais para servir como analogia.

i) PROTEÇÃO AO CRÉDITO: Base que somente existe aqui no Brasil, o objetivo do legislador na LGPD foi evitar que titulares de dados pessoais se utilizem de uma brecha legislativa para criarem mecanismos de escaparem de cobranças por dívidas contraídas, ou seja, se é devedor é e está inscrito nos órgãos de proteção ao crédito é para garantir que o credor seja pago, pois, caso contrário, o credor ficaria sem mecanismos de cobrança ou de concessão de crédito se o beneficiário é mal pagador.

j) LEGÍTIMO INTERESSE: Não é carta coringa. Assim como o consentimento, devendo ser utilizada somente quando não houver outra base legal aplicável ao caso. O art. 10 da LGPD determina que o legítimo interesse do controlador somente possa fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a apoiar e promover atividades do controlador e; proteger, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais.

Aqui o controlador deve observar pontos para aplicar essa base:

- Meu interesse é realmente legítimo?
- Meu interesse é necessário?
- Meu interesse está equilibrado?
- Meu interesse está salvaguardado?

6) APLICAÇÃO DOS PRINCÍPIOS E DAS BASES

A regra é uma base legal para cada finalidade.

Devem estar presentes todos os princípios.

Cada finalidade deve ter somente uma base legal, sendo esta a mais adequada para a finalidade que vai embasar.

Caso o tratamento de dados venha a ser adequado pela LGPD, mais estes dados já estão em uso e de posse da empresa, não precisará de consentimento se tiver uma base legal que a justifique. Porém, nunca é demais obter o termo de consentimento e, dispor as condições de tratamento daquele dado, de forma transparente e explicativa.

Para o tratamento de dados, a sugestão para os leigos ou mesmo utilizada por empresas experts no tratamento de dados é a nuvem, ou seja, utilizar-se de soluções digitais para aplicação e adequação da LGPD é uma das escolhas mais acertadas. A digitalização do escritório, seja qual for sua função e atividade desempenhada é uma forma de promover rastreabilidade às operações de tratamento de dados, e, aqui a nuvem é mais que uma ferramenta, é uma aliada.

7) COMO DESCARTAR DADOS

Para o descarte de dados, sejam físicos ou em mídias, temos níveis de relevância, sugerindo o quadro confeccionado pela Tilibra Express e que segue:

	Nível 01: Quando sua divulgação não causa nenhum dano para a organização ou o titular dos dados.	**Nível 02:** Quando a divulgação causa pequenos constrangimentos ao titular, bem como inconveniência operacional interna na Organização.	**Nível 03:** Quando a divulgação tem impacto significativo, porém reduzido sobre a privacidade e segurança do titular e, consequentemente, nas operações e objetivos da Organização.	**Nível 04:** Quando a divulgação tem sério impacto sobre a segurança e privacidade do titular e também nos objetivos do uso dos dados pela Organização, cuja sobrevivência pode estar em risco no caso de vazamento.
Mídia digital	Sem restrições	Eliminação feita somente dentro das áreas da Organização.	Dispositivos que contenham informações sensíveis devem ser destruídos fisicamente ou as informações contidas nos mesmos devem ser apagadas por meio de técnicas que tornem as informações originais irrecuperáveis.	Dispositivos que contenham informações sensíveis devem ser destruídos fisicamente ou as informações contidas nos mesmos devem ser apagadas por meio de técnicas que tornem as informações originais irrecuperáveis.
Mídia impressa	Sem restrições	Eliminação realizada nas dependências da Organização, com a utilização de uma fragmentadora.	Convém que a fragmentação seja feita na área do setor responsável pelas informações que serão descartadas.	Convém que a fragmentação seja feita na área do setor responsável pelas informações que serão descartadas.
Arquivos aparelhos	Sem restrições	Excluir da pasta e/ou local arquivado.	Excluir da pasta e/ou local arquivado e da lixeira também.	Excluir da lixeira, dos dispositivos e adotar soluções tecnológicas visando garantir que as informações não sejam recuperadas em hipótese alguma.

8) PENALIDADES DA LGPD

Os agentes de tratamento que violarem as normas previstas na LGPD estarão sujeitos à aplicação de advertências, multas, sanções administrativas pela Autoridade Nacional, que são:

• Advertência, com indicação de prazo para adoção de medidas corretivas.

• Multa simples de até 2% (dois por cento) do faturamento da empresa, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, e limitada no total de R$50.000.000,00 (cinquenta milhões de reais) por infração.

• Multa diária, observado o limite previsto no item acima.

• A publicização da infração.

• Bloqueio dos dados pessoais aos quais se refere a infração até a sua regularização.

• Eliminação dos dados pessoais aos quais se refere a infração.

9) LGPD E DIREITO DO TRABALHO

A LGPD não foi projetada especificamente para as peculiaridades do trâmite de informações entre patrão e empregado. Seu alcance é o trânsito de informações dos cidadãos nas redes sociais, aplicativos, cadastros de clientes, mas a LGPD não excluiu as relações de trabalho do seu âmbito de aplicação (artigo 3º). Além disso, as relações de trabalho, e outras relações vizinhas à estas, como a prestação de serviços em geral, e-social, segurança e saúde do trabalho, educação, dentre outras, implicam, também, o trânsito de informações entre uma pessoa natural, o empregado ou prestador de serviços, e uma outra pessoa, natural ou física, que vem a ser o empregador.

Em alguns casos a empregadora acaba por ultrapassar os limites da privacidade, mas devemos nos atentar que é por prevenção ou por que há dispositivo legal que precisa ser aplicado.

Temos como exemplo a lei do caminhoneiro, na qual é necessário que o motorista faça o exame toxicológico, ou seja, é uma prevenção para resguardar o próprio motorista, a empresa, e, terceiros. Porém, não deixa de ser tratamento de dados sensíveis e, de ser necessária resguardar a privacidade.

O preenchimento do currículo virtual permite uma análise prévia do perfil e atinge muito mais do que deveria, pois, muitas vezes o examinador acaba por tratar o candidato dentro de critérios discriminatórios e não seletivo pela função.

O empregador também necessita repassar dados do contrato laboral para terceiros, órgãos públicos, seguradoras, agências financeiras, planos de saúde, clínicas ocupacionais, etc.

Ou seja, observa-se que o tratamento de dados deve estar adequado com os princípios e bases legais, aplicando-se a LGPD.

9.1.) LGPD E O TELETRABALHO

Alguns pontos devem ser observados, vejamos hipóteses de ação:

a) Independentemente de o equipamento ser particular ou cedido pelo empregador, deverá existir um protocolo para armazenamento de informações relacionadas à prestação de serviços. Passo a passo bem descrito para que os dados dos clientes e funcionários não se percam no dispositivo eletrônico usado, ou seja, acessado e tratado indevidamente, causando consequentemente algum dano.

b) Priorizar um sistema de armazenamento na nuvem (por procedimentos de segurança como a anonimização e criptografia de dados), tendo um maior controle dos dados do contratante, menor vínculo e acesso desnecessário aos dados pertencentes ao contratado.

c) Implementar rotina semanal/mensal em que o contratado se compromete a eliminar eventuais dados salvos no aparelho particular em razão do trabalho.

d) Prever no contrato de trabalho, ou no atual cenário da pandemia, promover termo aditivo, a previsão do tratamento de dados, sob pena de responsabilização.

10) LGPD E *E-SOCIAL*

No que diz respeito ao programa *e-social* não haverá alteração.

Ou seja, o programa não sofrerá qualquer alteração das já previstas na normatização correspondente, entretanto, o tratamento de dados sim, especialmente no que tange aos dados sensíveis do trabalhador.

Dever-se-á transmitir somente os dados indispensáveis e estritamente necessários e exigidos pelo programa, destacando-se autorização expressa/consentimento do trabalhador. Observe-se que aqui caberia a base da obrigação legal, pois o *e-social* possui regramento próprio, porém, indica-se que o colaborar seja cientizado no ato da contratação ou por termo aditivo da necessidade de serem tratados os dados, evitando-se, assim, danos e surpresas.

11) LGPD E SAÚDE OCUPACIONAL

O artigo 3º da LGPD dispõe a aplicação dos artigos à qualquer operação de tratamento de dados, seja físico ou virtual, sem ressalva ao contrato de trabalho, como vimos no item anterior, bem como, consequentemente à SST – Segurança e Saúde do Trabalho, pois não estão nas hipóteses excedentes do artigo 4º da LGPD.

Portanto, se não há previsão permissiva ou proibitiva na LGPD, e, no geral se aplicará na tramitação de qualquer dado, exceto sem fins lucrativos, sugere-se que sindicatos e empresas convencionem e prevejam questões específicas sobre o tratamento de dados em acordos convencionais e convenções coletivas de trabalho, pautando-se no artigo 611 A da CLT e artigo 7º, XXVI, CF.

Observe-se que a LGPD é norma de caráter amplo e genérico, não direcionada especificamente às relações de trabalho e decorrentes (*e-social* e SST), mas, os dados que envolvem essas relações devem ser tratados nos termos da LGPD. Ressaltando-se se tratar na maioria de dados sensíveis, necessitando ainda mais de cuidados.

Então, dai a importância das CCT's e ACT's preverem pontos específicos da LGPD à relação de trabalho e assuntos decorrentes, tendo em vista que se sobressairiam à LGPD, evitando-se assim, problemas de tratamento de dados pelas empresas. Outrossim, é importante observar que não se pode ultrapassar ou ferir os princípios previstos no artigo 2º da LGPD.

Ainda, há de ser pontuado que no caso de documentação médica do trabalhador, devem-se observar os princípios e as bases legais, além, é claro, do sigilo aos dados médicos e de prontuário já previstos pelo Código de Ética Médica (Resolução 2217 de 27/09/2018), Lei 13787/2018 e Resolução CFM 1638/2002.

12) LGPD E ENSINO

Neste caso, pode haver dados normais e dados sensíveis.

Observe-se que aqui o ensino é desde alfabetização à capacitação, cursos, ensino superior, EAD ou presencial, etc.

Dentre as 10 bases legais, o consentimento não será a principal e única a ser usado nestes casos, podendo a instituição buscar a base legal mais adequada ao contexto no tratamento de dados de seu estabelecimento. Exemplos: legítimo interesse, cumprimento de obrigação regulatória e obrigações oriundas de contratos.

Perante a lei brasileira, é obrigatório o consentimento dos responsáveis legais para o tratamento de dados pessoais para todos os menores de 18 anos, nos termos da definição trazida pelo ECA - Estatuto da Criança e do Adolescente.

Dra. Valtielli T. Coutinho
advogada@valtielli.com.br
+55 (41) 9 8803-9233

Valério Wagner
valeriowagner@protecnicapr.com.br
+55 (41) 9 9923-3414