COMISSÃO DE PRIVACIDADE E PROTEÇÃO DE DADOS

Proteção de Dados Pessoais nas Relações de Trabalho

Novembro 2021

APRESENTAÇÃO

Fundada em 22 de janeiro de 1932, a OAB SP é a maior Secional do Brasil, com mais de 450 mil profissionais inscritos, quase 5 mil estagiários e 33 mil sociedades inscritas.

Mantém 120 comissões atuantes, entre permanentes e especiais, que desenvolvem trabalhos de estudo e aperfeiçoamento da legislação, além de zelar pela Advocacia paulista e pelos cidadãos.

São 915 postos de atendimento espalhados por todo o Estado, incluindo a Seccional e as 253 Subseções, e 241 pontos de Certificação Digital.

A entidade promove, com exclusividade, a representação, defesa, seleção e disciplina da Advocacia.

Ao defender a Constituição, a ordem jurídica do Estado Democrático de Direito, os direitos humanos e a justiça social, contribui com a consolidação das instituições democráticas e da cidadania brasileira.

Presidente: Caio Augusto Silva dos Santos

Vice-Presidente: Ricardo Luiz de Toledo Santos Filho

Secretário-Geral: Aislan de Queiroga Trigo

Secretária-Geral Adjunta: Margarete de Cássia Lopes

Tesoureira: Raquel Elita Alves Preto

APRESENTAÇÃO

A Comissão Privacidade e Proteção de Dados da OAB/SP tem como objetivo representar foro de discussão técnico-jurídica sobre a Privacidade e Proteção de Dados Pessoais, com foco profissional, legislativo, acadêmico e social.

Da mesma forma visa fomentar a interação e a contribuição entre profissionais, estudiosos, outras comissões, autoridades e reguladores.

Ainda, gerar pesquisa, conteúdo, orientações, campanhas educativas, além de criar e/ou monitorar indicadores, propostas e sugestões para melhoria e aperfeiçoamento do tema.

Busca aproximar e fortalecer laços institucionais, especialmente junto à ANPD e CNPDP e exercer papel de referência acerca da matéria, perante seus membros e demais advogados inscritos na OAB/SP.

Presidente: Patrícia Peck Garrido Pinheiro

Vice-Presidente: Marcelo Henrique Lapolla Aguiar Andrade

1º Secretário: Marcelo Xavier de Freitas Crespo

2ª Secretária: Gabriela de Avila Machado

Secretária Executiva: Sandra Avella Ramirez

Secretário Adjunto: Felipe Augusto Mancuso Zuchini

EQUIPE DE ELABORAÇÃO DA CARTILHA

Esta Cartilha foi elaborada e produzida por integrantes da Comissão de Privacidade e Proteção de Dados da OAB/SP.

Grupo de Trabalho: LGPD nas Relações de Trabalho

Coordenação:
Caren Benevento Viani

Contribuições:
José Edilson Lira Junior
Juliana Neves Crisostomo
Diana Cristina Rosa Santana
Mario Baldir Rodrigues Filho
Fernanda Dutra Vieira Lopes

ÍNDICE

A PROTEÇÃO DE DADOS PESSOAIS NAS RELAÇÕES DE TRABALHO

Em termos globais, a proteção de dados dos indivíduos é um tema que está presente em leis, regulamentos e normas dos principais países democráticos desde a década de 1970.

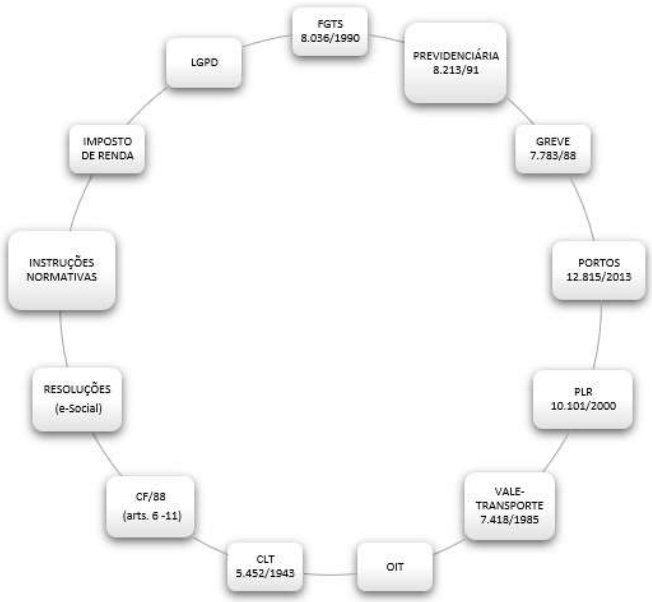
O Conselho Europeu e a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) tiveram protagonismo na criação de princípios e diretrizes para o tratamento de dados pessoais, inclusive sobre transferência internacional e processamento automático.

Em 25 de maio de 2018 entrou em vigor o regulamento europeu de proteção de dados – *General Data Protection Regulation* (GDPR) – considerada a norma mais abrangente sobre proteção de dados, alcançando todos os cidadãos dos estados-membros pertencentes à União Europeia.

No Brasil, a proteção dos dados pessoais está regulamentada na recém promulgada Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709 de 14 de agosto de 2018 - alterada pela redação dada pela Lei nº 13.853 de 2019 e que entrou, efetivamente, em vigor em 18 de setembro de 2020.

Essa legislação buscou subsídios no regulamento europeu e se propõe a proteger os dados dos cidadãos brasileiros em todo o território nacional. A LGPD trouxe em seu escopo a garantia de direitos aos titulares de dados e, em contrapartida, criou uma série de obrigações a serem cumpridas pelas empresas e entidades públicas e privadas, agentes de tratamento de dados.

Neste trabalho, visamos clarear a importância da adequação das empresas à LGPD, dando maior ênfase aos dados pessoais dos empregados, coletados e tratados para a finalidade da manutenção da relação de trabalho.
Exemplo de leis aplicáveis ao universo trabalhista:



DEFINIÇÕES

DADO PESSOAL

Informação relacionada à pessoa natural identificada ou identificável.

DADO PESSOAL SENSÍVEL

Dado pessoal sobre origem racial ou étnica, convicção religiosa, 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.

CONTROLADOR

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

OPERADOR

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

AGENTES DE TRATAMENTO

O controlador e o operador.

TRATAMENTO

Toda operação realizada com dados pessoais (coleta, armazenamento, compartilhamento, processamento, transmissão, acesso, utilização...).

ANONIMIZAÇÃO

Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

TITULAR

Pessoa natural a quem se referem os dados pessoais que são o objeto de tratamento.

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

USO COMPARTILHADO

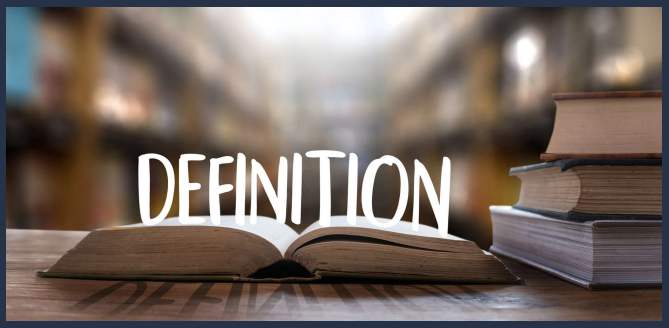
Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais.

CONSENTIMENTO

Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

ELIMINAÇÃO

Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.



DEFINIÇÕES

QUAIS SÃO OS FUNDAMENTOS DA LGPD?

A LGPD está fundamentada no respeito à privacidade; na autodeterminação informativa; na liberdade de expressão, de informação, de comunicação e de opinião; na inviolabilidade da intimidade, da honra e da imagem; no desenvolvimento econômico e tecnológico e a inovação; na livre iniciativa, concorrência e defesa do consumidor; nos direitos humanos, no livre desenvolvimento da personalidade, dignidade e no exercício da cidadania.

O QUE É TRATAMENTO DE DADOS PESSOAIS?

É toda operação realizada com dados pessoais (coleta, recepção, utilização, acesso, distribuição, processamento, armazenamento, eliminação...), tanto nos meios físicos como nos digitais (art. 1º LGPD), realizado por pessoa natural ou 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."

Isso representa que os dados pessoais são protegidos não somente nos meios físicos, mas, também, nos meios digitais.

E, além disso, estão elencados como agentes de tratamento de dados, não apenas as pessoas jurídicas, mas também as pessoas físicas, de direito público ou privado.

Os agentes de tratamento estão especificados na lei como CONTROLADOR e OPERADOR.

O primeiro é quem decide sobre o tratamento, e o segundo é aquele que apenas realiza o tratamento em nome do primeiro.

E O QUE SÃO DADOS PESSOAIS?

O artigo 5º, I, da LGPD diz que dado pessoal é qualquer informação relacionada a pessoa natural identificada ou identificável.

Podemos dizer que os dados que identificam uma pessoa são os dados comuns, como: nome completo, CPF, RG, CTPS, PIS/NIT. Há também os dados que podem identificá-la, como a geolocalização, endereço de IP, preferências de navegação e muitos outros que, se trabalhados em conjunto, podem chegar a um indivíduo.

DEFINIÇÕES

E os dados pessoais sensíveis, elencados no artigo 5º, II da LGPD, que são aqueles cujo tratamento pode resultar em algum tipo de discriminação do seu titular.

Eles estão definidos como:

- *dado pessoal sobre origem racial ou étnica;*
- *convicção religiosa;*
- *opinião política;*
- *filiação a sindicato ou a organização de caráter religioso, filosófico ou político;*
- *dado referente à saúde;*
- *vida sexual;*
- *dado genético ou biométrico, quando vinculado a uma pessoa natural.*

É importante esclarecer que os dados anonimizados, ou seja, aqueles que passam por um processo técnico que impossibilita a associação direta ou indireta a um indivíduo, perdem a proteção da LGPD.

Como exemplo, a anonimização de dados pessoais para fins de análise estatística.

E COMO OS DADOS PESSOAIS DEVEM SER TRATADOS?

Em primeiro lugar devem ser observados os princípios estabelecidos na LGPD.

Princípios

FINALIDADE

Realização do tratamento para propósitos legítimos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

ADEQUAÇÃO

Compatível com as finalidades informadas ao titular.

NECESSIDADE

Limitar o tratamento ao mínimo necessário para a realização de suas finalidades, evitando dados excessivos.

LIVRE ACESSO - Garantir a consulta facilitada.

QUALIDADE - Exatidão, clareza e relevância dos dados.

TRANSPARÊNCIA

Prestar aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

SEGURANÇA

Não há proteção de dados sem a utilização de medidas técnicas e administrativas aptas a protegê-los de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda e alteração.

PREVENÇÃO

A adoção de medidas de proteção de dados deve ser realizada previamente ao dano, buscando evitá-lo.

NÃO DISCRIMINAÇÃO

Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS

Não basta adotar medidas eficazes, é necessário demonstrá-las e comprovar a observância e o cumprimento das normas de proteção de dados pessoais

DEFINIÇÕES

E NAS RELAÇÕES DE TRABALHO, COMO OCORRE O TRATAMENTO?

O EMPREGADO também é titular de dados pessoais. No entanto, o CONTROLADOR dos seus dados é o seu EMPREGADOR, que pelos termos da CLT, art. 2º, é aquele que admite, assalaria e dirige a prestação pessoal dos serviços. Existe, portanto, um vínculo entre o empregado e o empregador que é o contrato de trabalho.

Essa relação contratual gera direitos e deveres para ambos, devendo-se respeitar as regras da Consolidação das Leis do Trabalho – CLT, da Constituição Federal – CF e das leis esparsas relativas ao assunto, assim como a LGPD.

EMPREGADO PODE SER OPERADOR OU CONTROLADOR?

O Guia orientativo* para definições dos agentes de tratamento de dados pessoais e do encarregado, publicado em Maio de 2021 pela Autoridade Nacional de Proteção de Dados (ANPD), traz as definições e exemplos práticos de quem são os controladores, operadores e controladores conjuntos.

Os empregados atuam em subordinação às decisões e comandos do empregador que é de fato o controlador, ou operador, não se confundindo, portanto, com a figura dos operadores de dados pessoais:

"Serão controladoras quando atuarem de acordo com os próprios interesses, com poder de decisão sobre as finalidades e os elementos essenciais de tratamento. Serão operadoras quando atuarem de acordo com os interesses do controlador, sendo-lhes facultada apenas a definição de elementos não essenciais à finalidade do tratamento.

O operador deve ser uma entidade distinta do controlador, isto é, que não atua como profissional subordinado a este ou como membro de seus órgãos.

Por outro lado, os funcionários atuarão em subordinação às decisões do controlador, não se confundindo, portanto, com os operadores de dados pessoais".

*Link: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf

ATRIBUIÇÕES DO RH

QUAL O PAPEL DO RH NO TRATAMENTO DE DADOS PESSOAIS DOS EMPREGADOS?

O setor de Recursos Humanos, independente se constituído como departamento próprio do empregador ou contratado para a prestação de serviços terceirizados, trata dados pessoais, inclusive sensíveis, para a execução de trabalhos que auxiliam na organização da empresa, compartilhando-os com outros controladores e operadores externos.

A fim de elucidar a criticidade das atividades executadas pelo setor de Recursos Humanos quando observado o tratamento de dados pessoais, faz-se necessário o detalhamento das principais atribuições do referido departamento.

Processo de Seleção

O processo de seleção requer o tratamento de inúmeros dados pessoais do candidato, inclusive, dados pessoais sensíveis, que são coletados através de formulários preenchidos por candidatos para entrevistas ou pelo envio de currículos. Esses dados são, muitas vezes, armazenados para processos seletivos posteriores.

Vale lembrar, que nessa fase são tratadas informações sobre a vida profissional pregressa do candidato e até mesmo salários.

Processo de Contratação

Na contratação, há um acréscimo de dados pessoais coletados e armazenados nas fichas cadastrais. Dados pessoais sensíveis, como aqueles relacionados à saúde do empregado, são coletados na realização dos exames admissionais, periódicos e demissionais.

As informações são compartilhadas com outros setores e empresas externas, como é o caso de seguradoras de vida, operadoras de plano de saúde, empresas que fornecem ticket-refeição, vale-alimentação e o próprio Estado, através do e-Social, dentre outras.

ATRIBUIÇÕES DO RH

Promoções

Ainda, dentro dos procedimentos deste setor, tem-se que há processos de promoções dos empregados.

Oportunidade em que, também, há coleta e armazenamento de dados pessoais, especialmente informações relativas às avaliações e feedbacks realizados, estatísticas de performance, evolução salarial, dentre outras que se relacionam ao empregado como titular de dados pessoais.

Regulamentos Internos

Dentro das responsabilidades que são geralmente atribuídas ao RH, encontram-se os processos relacionados à implementação de normas de convivência e relacionamento interno e externo, o que acaba gerando a criação de mídias e mecanismos corporativos.

Muitas vezes, utilizam-se de imagens de empregados com o objetivo de informar novidades da empresa e novas parcerias estabelecidas.

A adoção de treinamentos e de políticas de incentivo a prática de ginástica laboral, que são atividades focadas no bem estar geral e cumprimento das normas regulamentadoras, também requerem a captura de dados pessoais.

Negociações Coletivas

Não menos importante, são as tratativas de negociações coletivas realizadas entre as empresas, geralmente, com a participação do RH, do departamento jurídico e dos Sindicatos representantes de categorias de trabalhadores.

Nestes casos, verifica-se o compartilhamento de listas contendo nomes e outros dados pessoais relativos aos empregados que estarão submetidos aquela Convenção ou Acordo Coletivo de Trabalho.

Conclui-se, portanto, que o setor de recursos humanos é uma das áreas mais críticas e sensíveis no que se refere ao tratamento de dados pessoais de empregados, sendo necessária sua adequação à LGPD, ainda que haja a terceirização integral de suas atividades.

BASES LEGAIS

E QUAIS SÃO AS PRINCIPAIS BASES LEGAIS QUE LEGITIMAM O TRATAMENTO DE DADOS PESSOAIS DOS EMPREGADOS?

EXECUÇÃO DE CONTRATO

A base legal da execução de contrato legitima o desenvolvimento de procedimentos, desde antes da efetiva contratação, como é o caso do processo seletivo, ainda que este seja realizado por empresa terceirizada, até a formalização e efetiva execução dos contratos de trabalho, com a coleta de dados pessoais que constarão nas fichas admissionais e de registro de empregados, contratos de trabalho, acordos de compensação de jornada e banco de horas, fornecimento de vale-transporte, vale-refeição, vale-alimentação, contratação de seguro de vida, plano de previdência privada, dentre outros benefícios que poderão ser ofertados pela empresa.

CUMPRIMENTO DE OBRIGAÇÃO LEGAL

A segunda base legal a ser citada se refere ao cumprimento de obrigação legal, uma vez que a coleta de dados pessoais é exigida para fornecimento de informações ao Governo, seja através de repasse no e-social, emissão de guias à Secretaria do Trabalho, INSS, ou outros órgãos estatais. Algumas normas também determinam o dever de guarda de documentos por determinado período de tempo.

EXERCÍCIO REGULAR DE DIREITOS EM PROCESSO JUDICIAL

Outra base legal que poderá ser utilizada para o tratamento de dados pessoais é o exercício regular de direitos em processo judicial, administrativo ou arbitral, inclusive, sob o fundamento dos princípios constitucionais da ampla defesa e do contraditório, que garantem a possibilidade de defesa de direitos, seja na qualidade de autor ou réu da demanda.

PROTEÇÃO DA VIDA OU DA INCOLUMIDADE FÍSICA

Outra base legal importante que legitima o tratamento de dados pessoais para proteção da vida e incolumidade física do próprio empregado ou de terceiro envolvido. Esta base poderá ser utilizada para justificar a captação de imagens através de câmeras instaladas nas dependências físicas da empresa, para garantir a segurança dos empregados, por exemplo.

CONSENTIMENTO - LEGÍTIMO INTERESSE

O consentimento do titular deve ser livre e inequívoco e o legítimo interesse do controlador não pode violar os direitos e liberdades dos titulares de dados. Portanto, o tratamento de dados pessoais legitimados por essas duas bases legais, requer uma análise mais aprofundada pelo controlador. A seguir, elas serão melhor exploradas.

BASES LEGAIS

CAUTELA NO USO DA BASE LEGAL DO LEGÍTIMO INTERESSE

O legítimo interesse do controlador é, de certa forma, relativo, e não pode se sobrepor aos direitos e liberdades do titular de dados. Para a regular utilização dessa base, é necessário a realização de um teste de proporcionalidade para que seja identificado o equilíbrio entre o interesse do controlador e a preservação dos direitos do titular.
Além de ser considerada uma base legal muito ampla, ainda é carente de maiores esclarecimentos por parte da Autoridade Nacional de Proteção de Dados.

POSSO USAR A BASE LEGAL DO CONSENTIMENTO NOS CONTRATOS DE TRABALHO?

O consentimento é a manifestação livre, informada e inequívoca em que o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Quando fornecido por escrito, deverá constar de cláusula destacada das demais e, alterando-se a finalidade, o titular deve ser informado para que forneça novo consentimento ou possa revogá-lo em definitivo.

Quanto a sua revogação, esta pode ser feita a qualquer momento, bastando a manifestação expressa do titular dos dados, por meio de procedimento gratuito e facilitado, ratificados os tratamentos realizados com base no consentimento anterior.

O consentimento requer certa formalidade, vejamos:
(i) deve ser livre, informado e inequívoco, ou seja, o titular dos dados deve "dar o seu consentimento" de forma autônoma, sem imposição por parte do controlador;
(ii) deve conter todas as informações pertinentes ao tratamento dos seus dados;
(iii) deve prever sua nulidade em caso de descumprimento desses requisitos por parte do controlador;
(iv) pode ser revogado a qualquer momento.

EM QUAIS CASOS A BASE LEGAL DO CONSENTIMENTO SERIA INDICADA NAS RELAÇÕES DE TRABALHO?

O poder diretivo exercido pelo empregador, em vários aspectos, anula a possibilidade do consentimento livre e inequívoco, fornecido por livre e espontânea vontade do titular.

Além disso, um dos maiores entraves para o seu uso é o fato de que ele pode ser retirado a qualquer tempo pelo titular, ainda que na constância de determinado vínculo de emprego.

No entanto, há situações dentro de uma relação de trabalho em que ele pode e deve ser usado como base legal, pois há momentos em que o titular é livre para decidir sobre o tratamento de seus dados, desde que o consentimento fornecido atenda aos requisitos do art. art. 8º, caput e § 1º da LGPD e informados acima.

A fim de exemplificar: a divulgação de evento interno de determinada empresa feita através de seu RH ou de qualquer outro setor empresarial, com a necessidade de utilização de imagem de determinados empregados.

Esta situação, diferentemente do uso da imagem para autenticação sistêmica ou até mesmo para inserção em crachá da empresa, não estaria legitimada nas bases legais de execução de contrato e demais bases legais, motivo pelo qual se faria necessário o colhimento de autorização expressa do titular para a utilização da imagem, inclusive com o consentimento específico acerca das efetivas finalidades do respectivo uso e prazo de validade.

Outro exemplo, são as comemorações dos aniversários dos empregados, motivo para que o empregador, dentro de suas iniciativas e atividades, ofereça uma confraternização ou divulgação dos nomes, fotos e datas em murais ou outros canais de comunicação pela empresa. Algumas pessoas podem se incomodar, por motivos pessoais e íntimos, como crença religiosa ou timidez, em comemorar o seu aniversário com exposição de foto e data.

Nestes casos, a base legal do consentimento é a melhor ou a única opção a ser utilizada.

E NO CASO DE MENOR APRENDIZ, É NECESSÁRIO COLETAR O CONSENTIMENTO?

Os aprendizes contratados pelas empresas, em sua maioria tem idade que varia entre 14 e 17 anos, e pela Lei Civil brasileira são considerados, absoluta ou relativamente incapazes, necessitando de um responsável legal para executar os atos da vida civil.

Sendo assim, é sabido que as empresas não poderão realizar a contratação direta de um menor sem que seus pais ou responsáveis legais prestem a devida assistência.

A LGPD destacou uma seção intitulada "Do Tratamento de Dados Pessoais de Crianças e de Adolescentes" (artigo 14), onde traz disposições especiais sobre como as empresas podem e devem tratar os dados de menores de idade, sempre visando o melhor interesse da criança e do adolescente.

Embora haja uma interpretação de que tenha conferido "capacidade" aos maiores de 12 e menores de 18 anos para o livre exercício de atos civis, tal fato não é verdade. Deve-se considerar sempre as regras da incapacidade absoluta e relativa, previstas nos artigos 3º ao 5º do Código Civil para assegurar a devida proteção dos dados pessoais dos menores de 18 anos.

TEMPO DE VIDA DO DADO PESSOAL DO EMPREGADO

COMO DEVE SER O RECEBIMENTO E O DESCARTE DOS CURRÍCULOS DE FORMA ADEQUADA À LGPD?

A fase pré-contratual na relação de trabalho, é tão importante quanto as fases contratual e pós-contratual. Nesse sentido, os currículos ganham uma atenção maior pelo fato de conterem uma quantidade generosa de dados pessoais, inclusive sensíveis, como: dados cadastrais, fotografia, raça, gênero e até opção religiosa.

Os currículos chegam às empresas pelos meios mais variados: e-mail, whatsApp, físico por entrega presencial em portaria ou recepção, ou através dos empregados.

O cenário ideal para as empresas seria padronizar a forma de recebimento de currículos, como criar uma plataforma ou aplicativo, para que os candidatos possam preencher um formulário pré-definido.

Além de ser um grande facilitador, seria melhor para gerenciar o volume de dados, uma vez que é possível atribuir apenas os campos para preenchimento das informações minimamente necessárias para a finalidade da contratação, atendendo, assim, ao princípio da necessidade.

O compartilhamento desses dados com terceiros deve seguir uma regra rígida de privacidade, sendo necessária a coleta do consentimento, para uma finalidade lícita e informada.

A utilização das técnicas de criptografia, pseudonimização e, a depender da finalidade do armazenamento, anonimização, são desejáveis para esse tipo de informação, a fim de evitar incidentes de privacidade.

O CONTROLADOR PODERÁ ARMAZENAR DADOS DE TRABALHADORES APÓS O ENCERRAMENTO DA RELAÇÃO CONTRATUAL?

A guarda de documentos após o encerramento da relação empregatícia, e consequentemente, o armazenamento dos dados pessoais do ex-empregado, seguem as disposições da legislação trabalhista e previdenciária.

O prazo legal para a guarda está vinculado ao prazo para a constituição de créditos, eventuais ações judiciais e por determinação da legislação.

Os artigos 7º, II e 16, I, da LGPD tratam da possibilidade de o controlador conservar em sua base os dados pessoais para cumprimento de obrigação legal ou regulatória.

E, ainda, é possível manter os dados para um possível exercício regular de direito em processo judicial, administrativo e arbitral, segundo determina o artigo 7º, VI, da LGPD.

Diante disso, mesmo após o término do contrato de trabalho, o controlador pode e deve manter os dados dos empregados que foram, antecipadamente, classificados nas bases legais mencionadas.

E QUAL O PRAZO DE RETENÇÃO DOS DADOS PESSOAIS APÓS O ENCERRAMENTO DO CONTRATO DE TRABALHO?

Documento	Prazo de guarda
Comunicação de Acidente de Trabalho (CAT)	5 anos
Comprovante de entrega da Guia da Previdência Social (GPS) ao sindicato representativo da categoria profissional mais numerosa entre os empregados	5 anos
Comprovante de pagamento de benefícios reembolsados pelo INSS	5 anos
Documentos relativos à retenção dos 11% sobre nota fiscal, fatura ou recibo de prestação de serviços	5 anos
Documentos que comprovem a isenção da contribuição previdenciária	10 anos
Folha de pagamento (fins exclusivamente previdenciários)	5 anos
Guia da Previdência Social (GPS)	5 anos
Lançamentos contábeis de fatos geradores das contribuições previdenciárias	5 anos
Perfil Profissiográfico Previdenciário (PPP)	20 anos
Salário-Educação - documentos relacionados ao benefício	5 anos
Salário-família - documentos referentes a concessão, manutenção e pagamento das cotas do salário-família	10 anos
Salário-maternidade - documentos relacionados ao benefício	5 anos
Sistemas e arquivos, em meio digital ou assemelhado das empresas que utilizam sistema eletrônico de dados para o registro de negócios e atividades econômicas, escrituração de livros ou produção de documentos de natureza contábil, fiscal, trabalhista e previdenciária.	5 anos
Acordo de compensação de horas*	5 anos
Acordo de prorrogação de horas*	5 anos
Adiantamento salarial - comprovante*	5 anos
Atestado de Saúde Ocupacional (ASO)	20 anos, no mínimo, após o desligamento do trabalhador.
Aviso-Prévio - comunicado*	5 anos
Autorização de descontos*	5 anos
Cadastro Geral de Empregados e Desempregados (CAGED)	5 anos a contar da data do envio
Carta com pedido de demissão*	5 anos
Comissão Interna de Prevenção de Acidentes (CIPA) - Processo eleitoral	5 anos
Contrato de trabalho*	indeterminado
Controle de ponto*	5 anos
Folha de pagamento*	5 anos

E QUAL O PRAZO DE RETENÇÃO DOS DADOS PESSOAIS APÓS O ENCERRAMENTO DO CONTRATO DE TRABALHO?

Documento	Prazo de guarda
Fundo de Garantia do Tempo de Serviço (FGTS) - depósitos e documentos relacionados**	30 anos
Guia de Recolhimento do Fundo de Garantia do Tempo de Serviço e Informações à Previdência Social (GFIP)**	30 anos
Guia de Recolhimento Rescisório do FGTS (GRRF)**	30 anos
Livros ou fichas de registro de empregados*	Indeterminado
Mapa de Avaliação Anual (SESMT)	5 anos
Programa de Controle Médico de Saúde Ocupacional (PCMSO)	20 anos
Programa de Prevenção de Riscos Ambientais (PPRA) - Histórico técnico de desempenho	20 anos
Recibo de pagamento de férias*	5 anos
Recibo de pagamento de salário*	5 anos
Recibo de pagamento do 13º salário*	5 anos
Recibo de pagamento de abono pecuniário*	5 anos
Recibo de entrega, relatório impresso ou cópia dos arquivos da RAIS	5 anos
Seguro Desemprego (Comunicação de Dispensa e Requerimento do Seguro-Desemprego)*	5 anos
Termo de Rescisão do Contrato de Trabalho (TRCT)*	5 anos
Vale-transporte - recibo e documentos relacionados ao direito*	5 anos

** Não há prazo legal. Nada impede que exista posicionamento diverso ao exposto, situação em que caberá ao empregador adotar o procedimento que julgar mais acertado.*

*** O Supremo Tribunal Federal (STF) declarou a inconstitucionalidade das normas que preveem prazo prescricional de 30 (trinta) anos para ações relativas a valores não depositados no Fundo de Garantia do Tempo de Serviço (FGTS).*

O STF entendeu que o FGTS é direito dos trabalhadores urbanos e rurais definido na Constituição Federal (art. 7º, inciso III) e, portanto, deve se sujeitar à prescrição trabalhista, de 5 (cinco) anos.

A decisão foi tomada na sessão plenária do STF em 13.11.2014, no julgamento do recurso extraordinário com agravo (ARE) 709212, mas até o presente momento não houve alteração na legislação do FGTS.

Fonte: <http://www.fiscosoft.com.br/main_online_frame.php?page=/index.php?PID=232063&key=4718627>

DADO PESSOAL SENSÍVEL

O tratamento de dados pessoais sensíveis exige uma tutela especial. No entanto, desde que respeitados os ditames legais, o tratamento é perfeitamente possível em determinadas situações.

É importante frisar a necessidade do consentimento livre e esclarecido, já tratado em outro tópico.

Outro aspecto importante consta no artigo 11, II, da LGPD, que dispõe sobre a legitimidade do tratamento desses dados sem o consentimento do titular, em diversas hipóteses:

a) cumprimento de obrigação legal;

b) tratamento compartilhado de dados necessários à execução de políticas públicas;

c) realização de estudos por órgão de pesquisa;

d) exercício regular de direitos, inclusive em contrato e em processo;

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde;

g) garantia da prevenção à fraude e à segurança do titular.

A norma vislumbrou tais possibilidades, pois não seria possível a prestação dos serviços e sua respectiva contrapartida se não houver a coleta desses dados, como por exemplo, nos casos de compartilhamento através do e-Social da origem racial do empregado contratado.

QUAIS OS CRITÉRIOS DE COLETA E COMPARTILHAMENTO DE DADOS PARA CONTRATAÇÃO DE SEGURO SAÚDE PARA O EMPREGADO E SEUS DEPENDENTES?

Na maioria dos casos há um corretor de seguro saúde que faz a intermediação dessa relação contratual. É fundamental que todos os envolvidos nessa relação tenham estabelecido práticas adequadas às regras da LGPD.

Nestes casos, os agentes de tratamento são: o corretor que faz a intermediação, a seguradora do plano de saúde e o empregador.

Em toda essa cadeia de compartilhamento, a privacidade do empregado deve ser preservada.

E não são apenas os dados do empregado que são compartilhados para contratação de seguro saúde. Os dados pessoais dos seus dependentes também fazem parte dessa rede de informações, o que inclui dados de crianças e adolescentes.

COMPARTILHAMENTO

A LGPD se manifesta sobre o tratamento de dados pessoais de menores. O artigo 14 da Lei diz que o tratamento de dados pessoais de crianças e adolescentes deve ser realizado no "melhor interesse" e o § 1º complementa, atribuindo o requisito do consentimento do responsável para a realização do tratamento de dados de crianças.

Assim, convém pontuar dois pontos relevantes: o primeiro é o conceito de criança e adolescente e o segundo é o "melhor interesse".

O Estatuto da Criança e do Adolescente (ECA) define criança como a pessoa de até 12 anos de idade incompletos e, adolescente, a pessoa entre 12 e 18 anos.

A LGPD requer o consentimento dos pais quando se tratar de dados pessoais de criança, ou seja, do menor até 12 anos incompletos.

O Considerando 38 do General Data Protection Regulation (GDPR) fala, expressamente, sobre o "melhor interesse" da criança: "As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais (...).

Feitas tais observações, é oportuno apurar a base legal adequada para legitimar a coleta dos dados pessoais para contratação de planos médicos, tendo em vista a necessidade de coletar dados pessoais sensíveis como os relacionados à saúde.

COLETA DOS DADOS PESSOAIS PARA CONTRATAÇÃO DE PLANOS DE SAÚDE.

O artigo 11 da LGPD, que regulamenta o tratamento de dados pessoais sensíveis, aponta as exceções que legitimam a coleta desses dados sem o fornecimento do consentimento pelo titular:

a) cumprimento de obrigação legal
b) tratamento compartilhado de dados necessários à execução de políticas públicas
c) realização de estudos por órgão de pesquisa
d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral
e) proteção da vida ou da incolumidade física do titular ou de terceiro
f) tutela da saúde
g) garantia da prevenção à fraude

Há casos em que a obrigação do fornecimento de plano médico está inserida na Convenção Coletiva da categoria do empregado e, portanto, há um dever legal a ser cumprido.

Por outro lado, quando não houver essa exigência, o plano pode ser oferecido por mera liberalidade do empregador e, uma vez aceito pelo empregado, o fornecimento passa a ser obrigatório para executar o contratado.

Desta forma, são duas possibilidades de bases legais: cumprimento de obrigação legal e execução do contrato.

Considerando que a execução do contrato não está prevista como base legal que poderia afastar o consentimento como excepcionado pelo artigo 11 da LGPD, o consentimento livre

Inclusive, o acesso aos dados de saúde, desde que utilizados para uma finalidade legítima, determinada e informada, trará benefícios ao titular de dados, que é a preservação da sua saúde. Isso não significa que a empresa poderá ter acesso ao prontuário médico do empregado.

O código de ética médica (Resolução CFM 2217/2018 art. 73) proíbe que o médico revele "fato de que tenha conhecimento em virtude do exercício de sua profissão, salvo por motivo justo, dever legal ou consentimento, por escrito, do paciente".

E a CLT acrescenta que "o resultado dos exames médicos, inclusive o exame complementar, será comunicado ao trabalhador, observados os preceitos da ética médica" (art. 168 § 5º). Neste sentido, é necessário verificar o que diz o artigo 11 da LGPD.

O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;
(...)

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

O controlador dos dados pessoais sensíveis é o médico e, portanto, há uma dicotomia entre o dever de cumprir uma obrigação legal e a observância do sigilo médico previsto no Código de Ética Médica, uma vez que o compartilhamento dos dados pessoais sensíveis partirá do médico do trabalho e não da empresa.

Assim, o que se pretende demonstrar é que o empregador tem como finalidade e necessidade o tratamento de dados relativos à saúde para cumprir a obrigação legal da preservação da vida do empregado.

No entanto, a necessidade de compartilhamento dessas informações deve ser analisada caso a caso, bem como a definição das bases legais.

O EMPREGADOR PODE EXIGIR A CARTEIRA DE VACINAÇÃO DO EMPREGADO?

Considerando as diretrizes do capítulo V da CLT e as Normas Regulamentadoras mencionadas acima, o empregador pode exigir que o empregado forneça a carteira de vacinação para controle da COVID-19 dentro do ambiente de trabalho.

O interesse coletivo, neste caso, deve prevalecer, assim como é dever do empregador obter parâmetros para o gerenciamento dos riscos ocupacionais.

Em abril de 2021 o Ministério Público do Trabalho editou a nota técnica 04/2021 considerando a COVID-19 um risco biológico existente no local de trabalho.

e esclarecido, não somente do titular empregado, mas também de seus dependentes, é necessário. E essa regra deve ser aplicada a todos os envolvidos - empregado, cônjuge, criança e adolescente – não devendo prevalecer os critérios de idade acima apontados, tendo em vista tratar-se de dados pessoais sensíveis.

Assim, o empregado responsável pela criança pode consentir com a coleta dos dados relacionados à saúde, legitimando o seu tratamento. No entanto, se a base legal for o cumprimento de obrigação legal, o consentimento não será necessário.

É evidente que a escolha da base legal deve considerar a análise pontual de cada operação de tratamento de dados pessoais e as suas peculiaridades para que seja a mais assertiva.

QUAIS OS CRITÉRIOS DO TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS PARA CUMPRIMENTO DE OBRIGAÇÃO LEGAL?

O capítulo V da CLT, intitulado DA SEGURANÇA E DA MEDICINA DO TRABALHO traz dispositivos que vinculam as empresas a cumprirem normas, códigos e regulamentos sanitários que tenham como propósito preservar a segurança e a saúde do trabalhador.

O artigo 157, nos incisos I e II, diz que cabe às empresas (I) cumprir e fazer cumprir as normas de segurança e medicina do trabalho, (II) instruir os empregados, através de ordens de serviço, quanto às precauções a tomar no sentido de evitar acidentes do trabalho ou doenças ocupacionais.

No mesmo sentido, o artigo 158, incisos I e II, estabelece que os empregados devem observar as normas de segurança e medicina do trabalho, inclusive as instruções de seus empregadores sobre as precauções a tomar para evitar os acidentes, além de colaborar com a empresa na aplicação das normas preventivas.

Estipula, ainda, no parágrafo único do mesmo artigo 158, que constitui ato faltoso do empregado a recusa injustificada em observar as instruções expedidas pelo empregador.

Recentemente, a Comissão Tripartite Paritária Permanente, instância de discussão para construção e atualização das normas regulamentadoras, alterou as Normas nº 1 (Disposições Gerais e Gerenciamento de Riscos Ocupacionais), nº 7 (Programa de Controle Médico de Saúde Ocupacional) e nº 9 (Programa de Prevenção de Riscos Ambientais). As alterações entrarão em vigor a partir de 03 de janeiro de 2022.

Tais alterações tiveram como objetivo modernizar o processo de apuração dos riscos ocupacionais, integrando as NR's num programa capaz de identificar e gerenciar os riscos físicos, químicos, biológicos e ergonômicos, atribuindo como primeira fase, os processos de identificação, avaliação e inventário dos riscos e, como segunda, os controles e plano de ação.

Dentro desse processo, os exames médicos admissional, periódicos e demissional realizados pelos empregados, ocupam o papel de controle. São os diagnósticos que irão orientar as empresas sobre a eficácia das medidas implementadas de preservação da saúde do trabalhador.

COMPARTILHAMENTO

CONSIDERANDO que a COVID-19 é um risco biológico existente no local de trabalho, e, a despeito de ser pandêmica, não exclui a responsabilidade do empregador de identificar os possíveis transmissores da doença no local de trabalho e as medidas adequadas de busca ativa, rastreio e iso - lamento de casos, com o imediato afastamento dos contatantes, a serem previstas no Programa de Controle Médico de Saúde Ocupacional, elabo - rado sob responsabilidade técnica do médico do trabalho, nos termos da alínea "d" do item 4.12 da NR 04);

(...)

O GRUPO DE TRABALHO – GT COVID-19 - DO MINISTÉRIO PÚBLICO DO TRABALHO insta os órgãos da administração pública direta e indireta, unidades e serviços de saúde, empresas, pessoas jurídicas, conselhos de saúde, no âmbito de suas atribuições, a adotar as seguintes medidas e diretrizes:

1. Incluir o risco biológico do SARS-CoV-2 no Programa de Prevenção de Riscos Ambientais - PPRA, identificando as funções em que há maior risco para contato e/ou para a disseminação do vírus no meio ambiente de trabalho, de acordo com os itens 9.1.5 c/c 9.1.5.3 e 9.3.3 da Norma Regulamentadora 9 - Programa de Prevenção de Riscos Ambientais (PPRA), do Ministério do Trabalho e Previdência. (...)

https://mpt.mp.br/pgt/noticias/nota-tecnica-do-gt-covid-19-no-04-2021-mascaras-1.pdf

Para a instituição, a estratégia profilática de vacinação, que visa à imunização do grupo de empregados, é uma das formas de controle de disseminação da doença dentro do ambiente de trabalho.

Portanto, estão presentes os princípios da finalidade e necessidade do tratamento de dados sobre vacinação dos empregados, cujas bases legais aplicáveis são: cumprimento de obrigação legal e proteção da vida ou da incolumidade física do titular.

O empregador deve agir com transparência e conscientizar seus empregados sobre a necessidade da vacinação, além de informar os motivos pelos quais esses dados serão coletados e tratados, com quem eles serão compartilhados e o prazo de retenção.

Por fim, esses dados devem ser armazenados adequadamente, estabelecendo regras de confidencialidade que restrinja o acesso somente a pessoas previamente autorizadas.

TERCEIRIZAÇÃO

COMO OCORRE O TRATAMENTO DE DADOS PESSOAIS DE EMPREGADOS NA TERCEIRIZAÇÃO?

Na terceirização de mão-de-obra, há de um lado a empresa de terceirização (empresa 1), que cede a mão-de-obra especializada, e de outro, a empresa contratante (empresa 2), que aloca o empregado da contratada em suas dependências para a execução dos serviços.

Ambas as empresas irão tratar os dados pessoais do empregado, porém, as finalidades do tratamento não são necessariamente as mesmas.

Por exemplo: a empresa 1 (empregadora direta) é quem faz o registro do empregado e o pagamento da remuneração e tributos. Os dados pessoais tratados com a finalidade de efetivar o registro e efetuar o pagamento estão dentro do gerenciamento de privacidade da empresa 1.

Em contrapartida, o empregado ficará alocado na empresa 2, a quem deverá fornecer dados biométricos para o acesso ao prédio, por exemplo. Esses dados serão tratados apenas pela empresa 2 e, portanto, não estarão presentes nos registros da empresa 1.

O que se busca alcançar com esses exemplos, é a demonstração de que a cessão da mão-de-obra não equivale por si só a um compartilhamento de dados pessoais. Mesmo havendo duas empresas envolvidas na contratação de um mesmo empregado não significa que os dados pessoais coletados por essas empresas terão a mesma finalidade de tratamento, o que coloca cada uma como controladora das informações que armazenar.

A empresa 1 é controladora dos dados pessoais coletados para registro. É ela quem deve estabelecer a base legal para manutenção desses dados após o término do contrato de trabalho. No entanto, ela não é controladora dos dados biométricos tratados pela empresa 2.

No processo de terceirização de mão-de-obra é dever de cada uma das empresas envolvidas, inventariar os dados e os seus fluxos e identificar as situações em que o compartilhamento é necessário e os respectivos papéis, seja como controladora, co-controladora ou controladoria conjunta e operadora dos dados pessoais de acordo com as finalidades.

O artigo 42 § 1º, II, da LGPD diz que:

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorrerem danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta lei.

E o artigo 43 da LGPD ressalta que os agentes de tratamento só não serão responsabilizados quando provarem:

I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

TERCEIRIZAÇÃO

Segundo a ANPD, embora a LGPD não explicite o conceito de controladoria conjunta ou co-controladoria de dados pessoais, é possível inferir que tal conceito esteja contemplado no sistema jurídico de proteção de dados.

A Autoridade buscou referência no direito europeu para definir controladoria conjunta:

O artigo 26 do Regulamento Geral de Proteção de Dados - RGPD (General Data Protection Regulation) diz o seguinte:

"Quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento, ambos são responsáveis conjuntos pelo tratamento. Estes determinam, por acordo entre si e de modo transparente as respectivas responsabilidades pelo cumprimento do presente regulamento, nomeadamente no que diz respeito ao exercício dos direitos do titular dos dados e aos respetivos deveres de fornecer as informações referidas nos artigos 13º e 14º, a menos e na medida em que as suas responsabilidades respectivas sejam determinadas pelo direito da União ou do Estado-Membro a que se estejam sujeitos. O acordo pode designar um ponto de contacto para os titulares dos dados."

Critérios adotados pela ANPD para verificar a existência de controladoria conjunta:

1. Mais de um controlador possui poder de decisão sobre o tratamento de dados pessoais;

2. Há interesse mútuo de dois ou mais controladores, com base em finalidades próprias, sobre um mesmo tratamento; e

3. Dois ou mais controladores tomam decisões comuns ou convergentes sobre as finalidades e elementos essenciais do tratamento.

Neste contexto, observa-se que o tratamento de dados biométricos para o acesso ao prédio da empresa 2 não se enquadra nos critérios de controladoria conjunta.

Apenas a empresa 2 tem o poder de decisão sobre esses dados, uma vez que está apenas na sua base, além de ser critério por ela estabelecido e para uma finalidade que julga legítima.

Também não há mútuo interesse, pois a coleta de dados para acesso ao prédio não é finalidade de tratamento da empresa 1. E, por último, não existe decisão convergente.

É certo que as finalidades para o tratamento dos dados pessoais do mesmo empregado serão diferentes, apesar dos dados pessoais envolvidos serem os mesmos em várias situações.

E QUANDO HÁ COMPARTILHAMENTO DE DADOS PESSOAIS NA TERCEIRIZAÇÃO?

No modelo de terceirização traçado acima, é esperado que a contratante da mão-de-obra terceirizada solicite à contratada os comprovantes dos pagamentos de remuneração e recolhimentos tributários previdenciários, para garantir que todos os pagamentos pertinentes àquela contratação estejam ocorrendo na data e forma corretas.

Esses comprovantes são documentos que contêm dados pessoais e, portanto, é um caso típico de compartilhamento de dados. A questão é identificar a base legal que legitime esse compartilhamento, uma vez que é uma obrigação contratual que nasce entre as empresas contratantes e não entre o empregado e a empresa.

QUAIS AS CONSEQUÊNCIAS QUE O RECONHECIMENTO DO VÍNCULO EMPREGATÍCIO TRARÁ À EMPRESA TOMADORA DE SERVIÇOS NO CASO DE PEJOTIZAÇÃO?

Haverá uma descaracterização das figuras dos agentes de tratamento de dados definidos no contrato de prestação de serviços?

Numa relação de prestação de serviços em que ambos tratam dados pessoais, seja em sistema de controladoria conjunta ou como controlador e operador, existe a figura de dois agentes de tratamento cada um com suas obrigações em relação aos dados pessoais tratados.

Exemplificando: numa situação em que um varejista contrata um vendedor autônomo, na forma de pessoa jurídica, que utiliza sua própria base de dados de clientes (mailing) para executar as vendas e, portanto, é controlador nessa relação, poderá haver uma alteração desse papel caso esse vendedor seja incorporado à estrutura jurídica do varejista, como resultado de um reconhecimento de vínculo empregatício.

Ainda que não tenha havido compartilhamento desses dados, existe o interesse econômico da oferta de produtos.

Na medida em que o vendedor assume a posição de empregado, o varejista, por outro lado, assume a posição de empregador e controlador daquelas informações.

O art. 2º, da CLT, prevê que o responsável pela atividade econômica é o Empregador, aquele que define as regras da operação e quais os riscos delas decorrentes serão aceitáveis ao negócio.

A Súmula 341 do STF reforça o entendimento de que o Empregador é responsável pelos atos culposos praticados pelo empregado, sendo que tal responsabilidade é objetiva.

Diante disso, a reintegração de um serviço previamente terceirizado demandará da controladora a atualização de seus registros de tratamento para refletir a nova condição.

PRIVACIDADE

DESCARTE

Quando verificado que não existe mais finalidade de tratamento, seja por rescisão do contrato ou desligamento do empregado, os dados deverão ser eliminados da base dos agentes de tratamento.

Se ainda persistirem finalidades posteriores, como retenção de dados para cumprimento de uma obrigação legal dos agentes de tratamento, ou seja, identificado que há necessidade de retenção para defesa em ação judicial ou administrativa, essas constatações devem ter sido registradas nos programas de gerenciamento de privacidade elaborados por ambos os agentes de tratamento.

Para os dados dos representantes legais de ambas as empresas, na hipótese de término do contrato, independentemente do motivo e, ausente qualquer base legal para manutenção dos dados pessoais, as partes devem se comprometer a eliminar de seus registros e sistemas todos os dados pessoais a que tiverem acesso ou que porventura venham a conhecer ou ter ciência em decorrência do contrato.

DIFERENÇA ENTRE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DA INFORMAÇÃO

É importante contextualizar a segurança da informação e sua importância na preservação da privacidade dos indivíduos.

A Segurança da informação se preocupa com a proteção dos ativos da informação: estrutura tecnológica (hardware/software/sistemas/aplicativos) estrutura física (armários, acessos) além dos dados em geral, que podem representar informações relativas ao negócio ou às pessoas jurídicas e físicas, sendo este último caso, os dados pessoais.

Há inúmeras informações dentro da estrutura da organização que merecem proteção, tais como dados financeiros, segredos de negócio, estratégias de marketing, ações promocionais ou lançamento de novos produtos.

E além destes, há os dados pessoais que identificam ou podem tornar um indivíduo identificado e que também precisam estar protegidos.

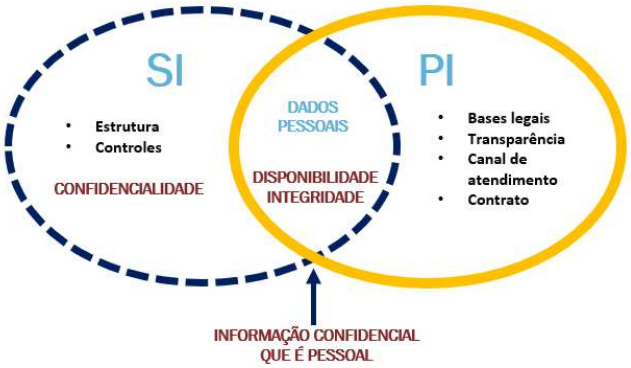
É importante salientar que nem toda informação que mereça algum grau de sigilo é uma informação pessoal.

A segurança da informação se preocupa em garantir a confidencialidade, disponibilidade e integridade de todas as informações, inclusive os dados pessoais.

PRIVACIDADE

A privacidade da informação se preocupa em garantir aos indivíduos o direito de controlar como e em qual extensão as informações sobre eles serão coletadas e posteriormente processadas.

Vejamos que há uma diferença importante entre essas duas modalidades de segurança. O quadro a seguir demonstra as suas diferenças e sobreposições.



Além de atribuir meios técnicos para manter a segurança dos dados pessoais coletados dos empregados, o controlador ainda deverá garantir o devido acesso e controle pelos titulares dos seus dados pessoais.

E O QUE É UM INCIDENTE DE PRIVACIDADE?

Segundo a ANPD, um incidente de privacidade é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como:

- acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda,
- qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

Essa mesma definição está contida no artigo 46 da LGPD, determinando que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais.

Vale afirmar que tais incidentes podem ocorrer no ambiente laboral e envolver dados pessoais de empregados.

A ANPD apresenta a seguinte orientação sobre o tema:

Avaliar internamente o incidente – natureza, categoria e quantidade de titulares de dados afetados, consequências concretas e prováveis. (Vide formulário de avaliação constante do sítio eletrônico da ANPD):

- Comunicar ao encarregado de tratamento de dados (Art. 5º, VIII da LGPD);
- Comunicar ao controlador, se você for o operador, nos termos da LGPD;
- Comunicar à ANPD e ao titular de dados, em caso de risco ou dano relevante aos titulares (Art. 48 da LGPD); e
- Elaborar documentação com a avaliação interna do incidente, medidas tomadas e análise de risco, para fins de cumprimento do princípio de responsabilização e prestação de contas (Art. 6º, X da LGPD).

MEDIDAS ADMINISTRATIVAS

QUAIS MEDIDAS ADMINISTRATIVAS SÃO NECESSÁRIAS PARA PROTEGER OS DADOS PESSOAIS DOS EMPREGADOS?

POLÍTICAS INTERNAS, PROCEDIMENTOS E CÓDIGO DE CONDUTA.

O empregado além de titular de dados pessoais também é aquele que acessa, recepciona, transmite, arquiva os dados de pessoas dentro da empresa. Diante disso, ele precisa estar consciente das implicações que o tratamento inadequado de dados pode causar à organização.

A LGPD (art. 50 § 2º, I, a) recomenda a elaboração de políticas e procedimentos internos que assegurem o cumprimento de normas de proteção de dados.

A adoção de boas práticas e governança são, inclusive, parâmetros de redução de sanções aplicadas pela ANPD.

Considerando que boa parte dos incidentes de segurança da informação têm em si uma ação humana envolvida, como por exemplo, abrir um e-mail corrompido, a desatenção da pessoa que abre o e-mail ou aplicativo é o fator determinante que desencadeia o ataque criminoso.

A proteção de dados pessoais é um tema a ser incorporado à governança corporativa, pois violações à privacidade podem gerar danos não apenas aos titulares, mas, também, à imagem e a reputação empresarial, afetando diretamente o negócio e seus stakeholders.

É necessária a formalização das regras sobre proteção de dados pessoais nas políticas internas.

Envolver a área de compliance e incluir no código de conduta os procedimentos a serem observados por toda a organização, inclusive estabelecendo as sanções em caso de descumprimento. O empregado deve ter acesso à essas regras no momento da contratação.

O contrato de trabalho pode fazer o apontamento de que o empregado toma ciência das normas internas na contratação, inclusive, celebrando o Termo de Confidencialidade, onde se compromete a não revelar informações, documentos e dados pessoais tratados pela organização.

Porém, não basta criar regras. É primordial conscientizar o corpo de empregados. Devem ser formulados textos com linguagem compreensível e divulgados a todos os empregados da organização.

Vide decisão: https://www.conjur.com.br/dl/1000612-0920205020043.pdf

MEDIDAS ADMINISTRATIVAS

Essas regras devem abranger ainda:

- normas de segurança
- definição de incidente e violação de dados pessoais
- padrões técnicos
- obrigações específicas para os diversos envolvidos no tratamento
- ações educativas
- mecanismos internos de supervisão e de mitigação de riscos
- transparência sobre o monitoramento de dispositivos de comunicação corporativo
- acesso a dados por empregados que trabalham à distância
- e outros aspectos relacionados ao tratamento de dados pessoais.

Todos dentro da organização devem saber que os meios de comunicação corporativos são monitorados. Aliás, a empresa deve ter o cuidado de não invadir os dispositivos pessoais dos empregados, fornecendo equipamentos próprios para serem utilizados no trabalho.

Há vasta jurisprudência nas Cortes Trabalhistas reconhecendo a legitimidade do empregador em monitorar as informações que circulam em emails e aplicativos corporativos.

Inclusive, a jurisprudência tem demonstrado que a punição do empregado que participou do incidente independe de dolo. Uma vez constatado que houve negligência em relação às regras de privacidade e proteção de dados corporativas, a punição é possível.

Ao criar a Comissão de investigação é essencial que os participantes celebrem Termo de Confidencialidade ou Non-Disclosure Agreement (NDA's), logo no início dos trabalhos, para garantir que os dados e as informações obtidas no processo não circulem indevidamente.

Durante um processo investigatório são coletadas inúmeras informações, inclusive dados pessoais sensíveis do investigado e de outras pessoas, como os entrevistados, por exemplo, capazes de violar a privacidade e a intimidade dos envolvidos.

O treinamento, sem dúvida, é o ponto forte para que as regras internas sejam incorporadas. Ele deve ser realizado em toda a organização e personalizado de acordo com o nível de acesso dos empregados, utilizando uma linguagem simples e clara.

E por fim, o monitoramento da efetividade do treinamento é outro fator importante, pois não apenas irá apontar as falhas como também determinar o espaçamento de tempo entre um treinamento e outro.

PRESTAÇÃO DE CONTAS

Apesar da relação assimétrica que existe entre empregado e empregador, tanto econômica, técnica, quanto informacional, é dever do empregador garantir aos empregados os direitos elencados no art. 18 da LGPD.

Estabelecer um canal de atendimento às requisições também dos titulares empregados é uma das formas de atender à autodeterminação informativa.

Além disso, ao atender ao princípio da transparência, irá garantir que o titular receba informações sobre o tratamento dos seus dados, bem como de seus respectivos agentes de tratamento, tudo de forma clara, precisa e facilmente acessível.

Essas técnicas informativas podem ser estruturadas através das políticas internas, que é a melhor forma de mostrar aos empregados as regras que o empregador segue sobre proteção de dados pessoais.

O CONTRATO DE TRABALHO DEVE INCLUIR A OBRIGAÇÃO DE DENÚNCIA POR PARTE DOS TRABALHADORES AO CONTROLADOR SOBRE INCIDENTES DE SEGURANÇA?

O artigo 47 da LGPD prevê que "os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término".

O artigo 48 da lei determina que:

"o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares".

Assim, para que o controlador possa atender a essa determinação em tempo hábil, é necessário que haja uma comunicação imediata sobre a ocorrência de um incidente que cause risco ou dano relevante ao titular.

A avaliação quanto ao risco e dano será feita por uma equipe ou profissional qualificado. Assim, importante que haja uma política de segurança da informação que possa comunicar aos trabalhadores o que é um incidente de segurança e quais as providências a serem tomadas caso isso ocorra.

Estabelecida em política e comunicada de forma adequada aos trabalhadores, sua infração será passível de punição, conforme a gravidade e prejuízos causados.

Importante considerar que o artigo 462, § 1º da CLT, permite o desconto na remuneração, em caso de dano causado pelo empregado, desde que esta possibilidade tenha sido acordada (prevista em contrato) ou na ocorrência de dolo do empregado.

Destaca-se, portanto, que o melhor meio para tratar temas relativos à proteção de dados de empregados é através das políticas e procedimentos internos.

CONCLUSÃO

O Brasil está amadurecendo no tocante a importância da privacidade de dados pessoais e caminha na compreensão de implementar os direitos dos titulares.

Enquanto a ANPD prossegue se estruturando e complementando a regulamentação do tema privacidade em nosso país, muitos casos já chegam aos tribunais, demandando dos magistrados a busca de referências em publicações das Autoridades Supervisoras da União Europeia.

Nesse intervalo de tempo, enquanto ANPD se prepara para a fiscalização com base na primeira resolução recém publicada em outubro de 2021, outras autoridades têm se sobressaído na defesa dos direitos dos titulares, com destaque para a SENACON, os PROCONs Estaduais e o Judiciário Trabalhista.

É de suma importância o acompanhamento da evolução do tema da privacidade nos Tribunais Trabalhistas, em virtude do diferente modelo de relação trabalhista vigente no Brasil, cuja tendência à proteção do trabalhador poderá desencadear decisões distintas dentro do Poder Judiciário, criando uma categoria privilegiada das demais em termos de proteção de dados pessoais.