

DPO é a sigla em inglês para o Encarregado de Proteção de Dados (Data Protection Officer), cargo que passou a ser obrigatório nas empresas com a entrada em vigor da Lei Geral de Proteção de Dados (LGPD). No Infracrev, esta função é ocupada pela Coordenadora Jurídica Maísa Carrasqueira.

Nessa entrevista, ela fala sobre como o Infracrev se preparou para cumprir a legislação e como são tratadas as informações dos participantes e assistidos do Instituto.

### **O que é a LGPD e qual o seu objetivo?**

**Maísa Carrasqueira:** A Lei Geral de Proteção de Dados – Lei nº 13.709, aprovada em 2018, entrou em vigor em setembro de 2020, em sua maior parte, restando para agosto de 2021 o início de vigência das sanções administrativas. Ela tem o objetivo de mudar a forma de funcionamento e operação das organizações, ao estabelecer regras claras sobre coleta, armazenamento e compartilhamento de dados pessoais, impondo uma padronização mais elevada de proteção e penalidades significativas para o descumprimento da norma legal.

### **Por que a LGPD foi criada?**

**Maísa Carrasqueira:** A LGPD foi criada especificamente para o controle e proteção de dados pessoais, buscando garantir todos os direitos possíveis dos titulares.

### **O que são considerados dados pessoais?**

**Maísa Carrasqueira:** De acordo com a LGPD, passa a ser considerada como um dado pessoal toda informação que permite identificar, direta ou indiretamente, um indivíduo que esteja vivo, tal como: nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, retrato em fotografia, prontuário de saúde, cartão bancário, renda, histórico de pagamentos etc.

### **O que mudou no Infracrev em função da LGPD?**

**Maísa Carrasqueira:** Todas as empresas que, direta ou indiretamente, lidam ou tenham contato com dados pessoais, em suas mais distintas formas, apresentações ou materializações, estão obrigadas a implementar controles internos e estruturas de governança, tendo em vista que a LGPD regula a questão de tratamento de dados, resultando no reforço de sua segurança. Para tanto, todas as empresas, inclusive o Infracrev, implementaram as medidas necessárias de adequação à regulamentação, de modo a atender às demandas e solicitações dos titulares de dados e mesmo da Agência Nacional de Proteção de Dados Pessoais (ANPD).

Importante ressaltar que esse processo de adequação foi idealizado e realizado respeitando e seguindo as melhores práticas do setor de previdência complementar, considerando o modelo de operacionalização interno, envolvendo as mais distintas medidas, desde simplificados ajustes, até um profundo mapeamento dos fluxos de dados, confecção de relatórios, bem como revisão de contratos celebrados com prestadores de serviços, contratos de trabalho, treinamentos com os empregados, alcançando a elaboração e desenvolvimento da nova Política de Proteção de Dados e de Privacidade, além da necessária nomeação do Encarregado (DPO – Data Protection Officer), que atua como um canal de comunicação entre os titulares de dados, o Infracrev e a ANPD, nos termos do art. 41 da LGPD.

### **O que o Infracrev e as empresas em geral devem observar ao tratar de dados dos seus clientes?**

**Maísa Carrasqueira:** É de suma importância observar que os dados pessoais tratados devem ser compatíveis com a finalidade informada. As empresas em geral devem utilizar apenas os dados estritamente necessários para alcançar as suas finalidades. Neste sentido, deverá ser ponderado o que é realmente essencial para a operacionalização e o que é apenas conveniente. Considerando

que a pessoa física titular dos dados tem o direito de consultar, de forma simples e gratuita, todos os dados que as empresas detiverem a seu respeito, impõe-se observar a forma como os dados são tratados e o prazo estabelecido para a sua guarda. Além de se preocuparem em cumprir integralmente a lei, as empresas devem ter provas e evidências de todas as medidas adotadas para o tratamento dos dados, de modo a demonstrarem a sua boa-fé e a sua diligência.

### **É preciso consentimento do cliente para que a empresa use seus dados?**

**Maísa Carrasqueira:** De acordo com o disposto no art. 7º da LGPD, é fundamental a solicitação do consentimento do titular para a utilização de seus dados, exceto nos casos relacionados no mencionado dispositivo legal. Em sendo assim, nessas hipóteses, as empresas não ficam obrigadas a solicitarem o consentimento do indivíduo para a coleta e tratamento de seus dados. No entanto, os dados coletados sem consentimento podem ser utilizados apenas para esses fins específicos. Logo, se o controlador quiser fazer outros usos dessas informações após a sua coleta, se não se encaixarem nessas exceções, o consentimento volta a ser obrigatório.

Cumprе ressaltar, ainda, que em se tratando de dados pessoais tornados manifestamente públicos pelo titular, exigir o consentimento deixa de ser obrigatório.

### **Quem tem seus dados pessoais protegidos pela LGPD?**

**Maísa Carrasqueira:** Conforme disposto no art. 17 da LGPD, “toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.” Portanto, o titular dos dados é a pessoa física a quem se referem as informações, sendo garantida a proteção a todos os seus dados pessoais, estejam eles em formato físico ou digital. Assim, a LGPD não alcança os dados titularizados por pessoas jurídicas, os quais não são considerados dados pessoais, para os efeitos da lei.

### **O que são dados pessoais sensíveis? E dados anonimizados?**

**Maísa Carrasqueira:** Os dados pessoais sensíveis são aqueles aos quais a LGPD conferiu uma proteção ainda maior, por estarem diretamente relacionados aos aspectos mais íntimos da personalidade de um indivíduo. Assim, de acordo com estabelecido pelo art. 5º, inciso II, da LGPD, são dados pessoais sensíveis aqueles relativos à origem racial ou étnica, convicção religiosa, opinião política, filiação à sindicato ou à organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa física.

Já um dado só é considerado anonimizado quando ele perdeu definitivamente a possibilidade de identificar uma pessoa física, quando não mais é associado a uma pessoa identificada. Em outras palavras, um dado anonimizado é um dado pessoal ou sensível que foi tratado para que suas informações não possam ser vinculadas ao seu titular original. Pela própria definição da lei, um dado anonimizado “perde a possibilidade de associação, direta ou indireta, a um indivíduo.”

### **Como é o processo para um dado pessoal se tornar anônimo?**

**Maísa Carrasqueira:** De acordo com o disposto no art. 5º da LGPD, a “anonimização é a 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.” Ou seja, a anonimização é o processo de fazer com que seja impossível identificar uma pessoa a partir do dado disponível.

Assim, deixando de ser dado pessoal, a informação fica fora do escopo de aplicação da LGPD. Ademais, registre-se por necessário que o processo de anonimização deve ser irreversível, na medida em que o dado não pode ser restaurado nem recuperado.

**Fonte:** [InfraPrev](#), em 28.09.2021.