POLÍTICA E MANUAL DE BOAS PRÁTICAS E GOVERNANÇA DE PROTEÇÃO DE DADOS PESSOAIS DA CERES – FUNDAÇÃO DE PREVIDÊNCIA

LEI GERAL DE PROTEÇÃO DE DADOS

1. INTRODUÇÃO

A presente Política e Manual de Boas Prática de Governança de Proteção de Dados Pessoais da Ceres – Fundação de Seguridade Social, em atenção à Lei Geral de Proteção de Dados – Lei nº 13.709/2018**,** tem por finalidade estabelecer os procedimentos e princípios de proteção de dados e ~~a~~ disciplinar aplicação dos dispositivos legais nas atividades de tratamento de dados desta Fundação.

O tratamento dos dados mencionados na presente Política de Proteção de Dados engloba os dados recebidos e enviados via documentos físicos e eletrônicos, por meio de gravação de voz e outros meios de tratamento citados na legislação de proteção de dados, de participantes, assistidos, beneficiários, empregados, terceirizados, contratados e visitantes.

2. DADOS PESSOAIS

Entende-se por dados pessoais qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável (titular dos dados). É considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social.

São exemplos de dados pessoais: nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via GPS, retrato em fotografia, prontuário de saúde, cartão bancário, renda, histórico de pagamentos, hábitos de consumo, preferências de lazer; endereço de IP (Protocolo da Internet) e cookies.

Os dados pessoal sensível são os dados 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.

3. TRATAMENTO DE DADOS PESSOAIS

Cada operador deve verificar quais os dados pessoais e sensíveis que são tratados em sua área para verificação do fundamento legal ou a necessidade de consentimento do titular e a identificação dos dados necessários para a atividade da Ceres.

Para tanto, se faz necessária a identificação dos dados de titulares que são tratados nas atividades de rotina de cada operador.

O operador deve identificar os dados que são realmente necessários para sua atividade de rotina e se estão vinculados ao termo de adesão, regulamento ou legislação (IN, Resolução, Portaria, Lei, decisões do Conselho Deliberativo, etc);

O operador deverá identificar os dados que possam ser eliminados por não serem necessários para sua atividade de rotina.

Necessário, ainda, que sejam identificados a necessidade e o tempo necessário pelo qual os dados devem permanecer arquivados na área.

Os riscos de vazamento desses dados devem ser, constantemente, identificados e avaliados para a adoção das medidas de mitigação e de comunicação.

4. COMPARTILHAMENTO DE DADOS COM OUTRAS GERÊNCIAS

As gerências da Ceres devem verificar os dados compartilhados com outras gerências e analisar o fundamento legal ou a necessidade de consentimento do titular para tanto.

Um registro de todos os dados deve ser atualizado periodicamente, no qual seja possível identificar de quais gerências recebeu os dados e com quais gerências os compartilha. Ademais, o compartilhamento de dados entre as gerências deve ter por fundamento ao termo de adesão, regulamento ou legislação (IN, Resolução, Portaria, Lei, decisões do Conselho Deliberativo, etc).

5. COMPARTILHAMENTO DE DADOS COM OUTRAS EMPRESAS

O operador deve verificar se faz o compartilhamento de dados com outras empresas e analisar o fundamento legal ou a necessidade de consentimento do titular para tanto.

É necessário que cada operador mantenha um registro de todos os dados que possui, de quem os recebeu e com que os compartilhou. Tal atividade de compartilhamento deve estar vinculada ao termo de adesão, regulamento, contrato em geral ou legislação (IN, Resolução, Portaria, Lei, decisões do Conselho Deliberativo, etc).

6. INDICAÇÃO E MONITORAMENTO DOS DADOS PELO ENCARREGADO

Nos termos da lei, a Ceres deve indicar e definir as atribuições da pessoa responsável como representante perante a Autoridade Nacional e terceiros, denominado de encarregado.

O encarregado deverá ter a rotina de acesso permanente às boas práticas de proteção de dados adotadas de todas as equipes da Ceres, compartilhando e trocando experiências quanto à rotina de proteção de dados.

Deve a Ceres, ainda, certificar-se de que o encarregado possua um canal para comunicação efetiva com a autoridade nacional e com os titulares dos dados.

7. MONITORAMENTE DE RISCOS À PROTEÇÃO DE DADOS

O encarregado deverá manter um relatório de vulnerabilidades e ameaças que possam gerar o vazamento de dados e verificar continuamente se as ações para evitar o vazamento são eficazes, devendo, para tanto, utilizar a estrutura técnica capacitada da Ceres, como: a Getec.

8. CONTRATOS – verificar a necessidade de aditivos nos contratos

As áreas da Ceres, juntamente com a gerência de administração, deverão incluir nos contratos, que devem ser sempre formalizados por escrito, a obrigatoriedade de dar o tratamento adequado aos dados pessoais que o contratado tiver acesso e comunicar imediatamente qualquer possibilidade ou o efetivado vazamento desses dados.

A Ceres deve ter o mesmo cuidado em relação aos dados recebidos do contratado, inclusive de seus sócios.

9. INFORMAÇÃO QUANTO À VULNERABILIDADE

Outra ação necessária da Ceres é certificar-se de informar aos titulares dos dados de todas as situações críticas nas quais seria possível ocorrer algum vazamento de dados e as providências adotadas para evitar que isso ocorra.

10. ARMAZENAMENTO, ACESSO E ATUALIZAÇÃO DE DADOS

Quanto ao armazenamento, o acesso e a atualização dos dados, a Ceres deve certificar-se de que o titular dos dados possua um canal para ter acesso a seus dados, a qualquer momento, e que ele possa, sempre que for necessário, atualizar tais dados, solicitar sua anonimização, não compartilhamento e exclusão, devendo o encarregado ser comunicado para avaliação e acompanhamento.

Os titulares devem ser esclarecidos das consequências decorrentes da anonimização, não autorização de compartilhamento ou exclusão de seus dados.

Os titulares devem também ter acesso ao encarregado para informar sobre a adoção de boas práticas para o compartilhamento de seus dados, com quais controladores seus dados foram compartilhados e as práticas de segurança adotadas para o tratamento e compartilhamento desses dados.

11. USO DE DADOS DE CRIANÇAS E ADOLESCENTES

O tratamento de dados de crianças e adolescentes deve se dar apenas com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

12. TRANSFERÊNCIA INTERNACIONAL DE DADOS

No caso de transferência de dados para outros operadores fora do Brasil, a Ceres deve certificar-se de que seu sistema informatizado seja capaz de proteger o compartilhamento de tais dados em conformidade com a lei de proteção de dados, o que deverá ser verificado, inclusive, em caso de armazenamento em nuvem. Nesses casos, deverá ser dada uma declaração da empresa com a qual a Ceres compartilha os dados. Quando for o caso, deverá ter autorização do titular do dado.

13. AÇÕES SOBRE POLÍTICA DE BOAS PRÁTICAS NA PROTEÇÃO DE DADOS

Algumas ações práticas devem ser tomadas e atualizadas frequentemente, como uma forma de política de boas práticas na proteção dos dados pessoais, as quais listamos abaixo:

13.1 - Manter relatório periódico descrevendo ações necessárias para o recebimento, compartilhamento, armazenamento e exclusão de dados e filtros de acesso a esses dados conforme os princípios da lei de proteção.

13.2 - Criar treinamento contínuo de atualização e implementação de boas práticas para os atuais e novos empregados e diretores.

13.3 - Manter uma política de atualização e de conscientização dessas boas práticas.

13.4 - Realizar esclarecimentos para os Conselheiros, inclusive sobre quais dados dos titulares poderão ter acesso.

13.5 - Utilizar ferramentas que possibilitem proteger os dados com os quais os operadores trabalham. Essas ferramentas podem ser informatizadas ou podem abranger práticas cotidianas de restrição de acesso, tais como:

a. acesso às pastas físicas: não deixar pastas abertas em cima de mesa sem a presença do operador e sempre guardá-las nas gavetas; telas de computador: bloquear o monitor toda vez que

se levantar de sua mesa ou quando outra pessoa se aproximar de sua mesa;
b. impressoras: não deixar documentos impressos na badeja;
c. localização física: quando for possível, remanejar empregados que mais utilizam dados dos titulares para locais com maior dificuldade de acesso.

13.6 - Eliminar dados recebidos na Ceres, de qualquer forma, de titular que não tiver amparo para o tratamento.

13.7 - Valorizar a diversidade e ser contra a discriminação por estado civil, etnia, gênero, idade, raça, cor de pele, origem, religião, deficiência, orientação sexual e condição social. Repudiar as atitudes abusivas contra a integridade moral e física, tais como assédio moral ou sexual, abuso de poder, agressão ou outro comportamento que possa ser considerado ofensivo, humilhante e discriminatório.

13.8 - Tratar os dados pessoais de participantes, assistidos, colaboradores, dirigentes e fornecedores com observância aos princípios de finalidade, adequação, necessidade, livre acesso, transparência, segurança, privacidade, não discriminação, prevenção e prestação de contas.

14. ACOMPANHAMENTO DO ENCARREGADO

O Encarregado deverá acompanhar, periodicamente, como definido pela Diretoria Executiva, a execução dessa política e realizar atividades para internalização das práticas de proteção de dados.

15. CONSIDERAÇÕES FINAIS

Esta Política de Privacidade e Proteção de Dados deve ser implementada, acompanhada e frequentemente atualizada para o cumprimento da legislação e para um bom desempenho da Ceres no intuito de tratar e bem proteger os dados pessoais de todos os titulares envolvidos nas atividades da Ceres.

FERNANDO NUNES SIMOES:26874008153

Assinado digitalmente por FERNANDO NUNES SIMOES:26874008153
DN: C=BR, O=ICP-Brasil, OU=Secretaria da Receita Federal do Brasil - RFB, OU=RFB e-CPF A1, OU=(EM BRANCO), OU=05194995000192, CN=FERNANDO NUNES SIMOES:26874008153
Razão: Eu sou o autor deste documento
Localização: sua localização de assinatura aqui
Data: 2020-12-29 19:18:50
Foxit Reader Versão: 10.0.0