Guia de Boas Práticas e Condutas para Proteção de Dados – CRIFFER LGPD

Introdução

O presente Guia de Boas Práticas e Conduta para Proteção de Dados tem como princípios e fundamentos os valores profissionais, sociais, éticos e morais, que orientam a realização das atividades desempenhadas interna e externamente pelos integrantes e colaboradores da empresa CRIFFER.

A CRIFFER, por meio deste regulamento interno, somado ao já existente Programa de Integração da TI, ratifica sua constante preocupação com a correta coleta, armazenamento, utilização e descarte de dados pessoais necessários à realização de determinadas atividades, uma vez que atenta ao interesse protetivo da Lei 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), aqui utilizada como parâmetro amplo e geral de atuação.

Além da LGPD, também as diretrizes estabelecidas nas demais legislações atinentes ao tema, como por exemplo, a Lei 12.965/2014 (Marco Civil da Internet), as regras gerais de responsabilidade civil e as disposições constitucionais, serão consideradas pela CRIFFER para o tratamento de dados, assim como, as políticas internas informadas pelos clientes, no que se refere aos seus respectivos interesses.

As regras, princípios e valores a seguir listadas têm o objetivo de garantir que os deveres de proteção de dados sejam incorporados e interpretados de maneira sistemática e com a menor subjetividade possível, visando criar um ambiente de trabalho profissional e com excelente padrão de conduta voltada ao tratamento de dados pessoais, sempre buscando atualizações e readequações necessárias aos procedimentos já instaurados.

I. Alcance

Art. 1º. Este Guia aplica-se, sem exceção, aos diretores, sócios, empregados, estagiários e colaboradores internos e externos da CRIFFER, doravante denominado “integrantes”.

Art. 2º. Todos os integrantes se comprometem a aderir aos seus termos e com estes anuir de forma ampla, obrigando-se a cumpri-los integral e fielmente em todo o seu teor, estando cientes, ainda, das regras estabelecidas na Lei 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) e sua responsabilidade solidária ou mesmo individual, de acordo com as situações concretas que se apresentarem.

Art. 3º. As pessoas físicas e jurídicas prestadoras de serviços, assim como os terceirizados que venham a exercer atividades nas sedes da CRIFFER, ainda que de forma temporária, serão informados do teor deste Código e solicitados a aderirem às suas normas.

Art. 4º. Aos integrantes, além da ciência acerca das disposições legais e orientações internas da CRIFFER, fica à disposição o acesso pessoal no ambiente da empresa e virtual (pelos canais internos de comunicação) aos membros do Comitê Permanente de Compliance, Instauração e Fiscalização das Diretrizes da LGPD, para esclarecimentos, sugestões e pesquisas conjuntas no intuito de cumprimento e melhorias aos procedimentos internos já adotados.

Art. 5º. O presente Guia será publicizado internamente da maneira mais ampla possível e será disponibilizado ao público geral em meio físico, na sede da empresa, bem como, por meio virtual no site da empresa e informativos em suas redes sociais.

II. Definições

Art. 6º. Em atendimento às denominações estabelecidas na LGPD, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - 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;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

IX - agentes de tratamento: o controlador e o operador;

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XI - 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;

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVII - 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;

XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

III. Comprometimentos Institucionais

Art. 7º. A CRIFFER nomeará o responsável pela política de proteção de dados (DPO), tornando pública e acessível esta informação, interna e externamente.

Art. 8º. A CRIFFER compromete-se a manter ativo o Comitê Permanente de Compliance, Instauração e Fiscalização das Diretrizes da LGPD, órgão interno criado para pesquisar, estabelecer, implementar e fiscalizar as políticas de proteção de dados, doravante denominado "Comitê LGPD", em conjunto com o corpo diretivo, a nível institucional.

Art. 9º. A CRIFFER buscará reiterar, registrar, divulgar, analisar e revisar periodicamente as políticas e os procedimentos de proteção de dados, inclusive no que se refere ao presente Código, buscando adequações, correições e melhorias àquelas implementadas, bem como, a realizar treinamentos periódicos ao público interno, tendo como tema a proteção de dados pessoais e a confidencialidade das informações.

IV. Princípios da gestão e segurança de dados

Art. 10. O tratamento de dados pelos integrantes da CRIFFER obedecerá aos seguintes Princípios Gerais previstos no art. 6º da LGPD:

I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Art. 11. Além dos referidos princípios previstos no artigo 6º, considera-se como princípios a Proatividade na busca pela preservação de dados que estejam sob seu domínio e a Anonimização dos dados, sempre que possível, de modo a reservar a privacidade do titular de dados.

Art. 12. Todos os Princípios acima elencados, sejam gerais ou específicos, devem ser interpretados e aplicados de maneira conjunta e sistemática, levando em consideração, de igual modo, os demais princípios gerais do direito.

V. Medidas de proteção de dados

V.I. Ações de proteção

Art. 13. A proteção de dados pessoais deve ser realizada em todas as etapas do serviço prestado pela CRIFFER, envolvendo, dentre outras, a concepção de sistemas internos, a análise prévia de sistemas externos eventualmente necessários para atividades da empresa, a realização de práticas comerciais, a contratação de pessoas, o relacionamento entre os Integrantes, o relacionamento com os clientes e, no que couber, com órgãos da administração pública.

VI - Respeito à privacidade do titular de dados: O tratamento de dados pessoais deve ser respeitoso e realizado, unicamente, de acordo com legítimo interesse da CRIFFER e do cliente, bem como, nos limites da autorização concedida.

Art. 14. O tratamento de dados pessoais deve ser realizado apenas no contexto do trabalho e do legítimo interesse da CRIFFER; essa determinação considera, de forma ampla, todos os dados pessoais tratados, estejam eles no sistema interno, nos sistemas específicos dos clientes, bem como, aqueles que venham a ser recebidos por meio físico ou virtual, de qualquer forma, armazenados.

Parágrafo único. Consideram-se contexto do trabalho e legítimo interesse da CRIFFER apenas o as medidas necessárias para elaboração de documento e/ou cumprimento da atividade informada previamente, preservando o interesse do titular dos dados e os limites de sua expressa autorização.

Art. 15. O tratamento de dados deve ser realizado considerando, não apenas a vedação da utilização indevida pelos Integrantes, mas, também, a promoção de medidas de segurança e atenção necessárias para preservar a incolumidade e restringir o acesso de terceiros.

Art. 16. Os integrantes, nos limites da atuação individual, devem manter níveis de segurança adequados à proteção de senhas e logins pessoais, não facilitando o acesso a tais informações em qualquer hipótese. Dentre outras medidas, é recomendado:

I - Evitar a utilização de uma única senha para vários logs diferentes;

II - Realizar periodicamente a troca de senha ou imediatamente, em caso de suspeita de que tenha sido comprometida;

III - Utilizar o botão “sair” ou “bloquear”, após finalizar sua navegação no sistema;

IV - Redobrar a atenção ao acessar logs pessoais em computadores ou redes de acesso público;

V – Evitar a utilização dos sistemas e canais de comunicação internos ou ainda aqueles externos de uso exclusivo da atividade da empresa em computadores pessoais ou redes de acesso público;

VI – Não compartilhar, seja por meio virtual ou dispositivo de armazenamento móvel, ainda que consigo mesmo, qualquer informação que possa conter dados pessoais, ainda que para realização de determinada atividade da empresa

Parágrafo Único – Em casos excepcionais, solicitar ao Gestor de Equipe e ao responsável do setor de Tecnologia da Informação, o fornecimento de “login” e/ou equipamentos adequados, de propriedade da empresa, para realização de tais atividades.

Art. 17. O uso do sistema, dos canais de comunicação e do e-mail corporativo é exclusivo para assuntos relacionados às atividades da empresa e poderão ser monitorados pelo setor de Tecnologia da Informação sempre que necessário.

Art. 18. Os integrantes deverão impedir o acesso a dados pessoais sob seu controle por terceiros quando estes estiverem em sua posse física e/ou digital, mantendo-os arquivados em suas estações de trabalho ou impedindo a visualização destes em seus monitores e demais pertencentes, físicos e tecnológicos, à exceção de exposição a demais integrantes internos da

CRIFFER para realização da atividade/atendimento da demanda para a qual foram disponibilizados, estimulando-se o diálogo e o debate estratégico/comercial, de modo que também atenda sua melhor utilização e/ou armazenamento.

Parágrafo único. A exposição de dados pessoais aos colaboradores externos é restrita ao seu fim específico, sendo vedada a comunicação de quaisquer outras informações que não sirvam ao fim pelo qual o colaborador foi designado e sempre que possível observará à anonimização.

Art. 19. Ao utilizar as impressoras, os documentos enviados para impressão devem ser recolhidos imediatamente, bem como, arquivos impressos indevidamente devem ser descartados adequadamente junto à fragmentadora de papéis.

Parágrafo único. Os integrantes deverão evitar a impressão e cópia indevida de arquivos, fazendo-o apenas quando necessário à atividade desenvolvida.

Art. 20. Os integrantes devem evitar circular em ambientes externos portando cópias (físicas ou digitais) de arquivos contendo dados pessoais relevantes, salvo se necessário para realização do trabalho e no contexto do legítimo interesse da CRIFFER.

Art. 21. O setor de Tecnologia da Informação (TI) da CRIFFER é o responsável exclusivo pela implementação dos procedimentos e controles técnicos de informática inerentes a esta Política de Segurança de Dados.

Art. 22. Os integrantes deverão comunicar ao Encarregado (DPO), com extrema urgência, de modo pessoal ou virtual, a ocorrência de qualquer situação que possa acarretar a violação ou o tratamento inadequado de dados pessoais, ainda que não tenha observado consequências.

V.II. Restrições expressas

Art. 23. Salvo no contexto do trabalho e do legítimo interesse da CRIFFER, é vedado aos Integrantes compartilhar externamente, mesmo que de forma meramente parcial, qualquer conteúdo da base de dados.

Art. 24. Nos mesmos termos, é vedado o compartilhamento, mesmo que interno, de dados considerados sensíveis, de acordo com o art. 5º, II da LGPD.

Art. 25. É vedado o compartilhamento interno ou externo de logins de acesso e senhas próprias entre os Integrantes da CRIFFER, cabendo àqueles que não possuam a informação ou o acesso necessário a essa informação, solicitar diretamente ao seu Gestor de Equipe e ao responsável pelo setor de Tecnologia da Informação, o qual, quando pertinente, lhe considera acesso e/ou buscará a informação solicitada.

Art. 26. É vedado, dentre outras medidas que possam comprometer a segurança da informação, realizar qualquer tipo de modificação nos softwares dos computadores, abrir as máquinas para realização de reparo, alterar as configurações de rede e da BIOS, sem a prévia autorização.

Art. 27. É vedado conectar dispositivos não autorizados na rede local, equipamentos de rede sem fio, equipamentos que permitam a ligação da rede interna da empresa à outra rede, que possam interferir na frequência/trabalho de operação dos equipamentos da Instituição ou que forneçam serviços de rede, como DHCP, NAT ou outros.

VI. Plano de resposta a incidentes de comprometimento de dados

Art. 28. Todos os riscos e incidentes que impliquem na violação da segurança de dados devem ser imediatamente reportados ao controlador, ao DPO e ao Comitê LGPD, que iniciarão o processo de resposta, obedecendo às seguintes etapas:

I - Identificação: detectar ou confirmar, de fato, a existência de um incidente de segurança ou violação de dados;

II - Coordenação e mitigação: verificar os danos causados pelo incidente e diagnosticar, de forma preliminar, a sua causa, adotando ações imediatas que possam resolver ou minimizar os riscos gerados pelo incidente;

IV - Comunicação à Autoridade Nacional: Nos termos do artigo 48 da LGPD, o Controlador deverá comunicar à Autoridade Nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante;

V - Investigação: coletar e analisar as evidências das causas do incidente;

VI - Conclusão: encerrar o tratamento do incidente, pela identificação da causa e/ou responsável pelo problema, bem com, das melhorias necessárias para evitar novas ocorrências. Eventualmente, remanescendo a ocorrência de danos ao titular, deve ser verificada a necessidade ou possibilidade de reparação.

VII. Infrações e desvios

Art. 29. A não conformidade com as políticas estabelecidas neste Código, inclusive as tentativas de contornar as determinações, manipulando ou evitando o processo determinado, podem resultar em ações disciplinares, inclusive o término do vínculo contratual ou empregatício.

Art. 30. O integrante que, por dolo ou culpa grave, der causa à violação da proteção de dados, responderá pelos danos e prejuízos correspondentes, seja diretamente perante o titular, seja perante à CRIFFER, mesmo que de maneira regressiva.

São Leopoldo, 20 de junho de 2022.

Comitê Permanente de Compliance, Instauração e Fiscalização das Diretrizes da LGPD da CRIFFER