

POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS**PL/DIREX-PDP/012/23/08-21****SUMÁRIO**

1. OBJETIVO	1
2. ABRANGÊNCIA.....	2
3. REFERÊNCIAS.....	2
4. DEFINIÇÕES.....	2
5. ATRIBUIÇÕES E RESPONSABILIDADES	4
5.1. Compete à Diretoria Executiva (Controladora):.....	4
5.2. Compete ao Encarregado de Proteção de Dados ou Data Protection Officer (DPO):	4
5.3. Compete ao Comitê de Privacidade de Dados:	4
5.4. Compete ao Escritório de Risco e Conformidade:.....	5
5.5. Compete ao Jurídico:.....	5
5.6. Compete à Gerência de Tecnologia da Informação:	5
5.7. Compete a todos os Colaboradores:	5
6. DIRETRIZES.....	6
6.1. Princípios de Proteção de Dados Pessoais	6
6.1.1. Legalidade, Transparência e Não Discriminação.....	6
6.1.2. Limitação e Adequação da Finalidade.....	7
6.1.3. Princípio da Necessidade (Minimização dos Dados)	7
6.1.4. Exatidão (Qualidade dos Dados)	7
6.1.5. Retenção e Limitação do Armazenamento de Dados	7
6.1.6. Integridade e Confidencialidade (Livre Acesso, Prevenção e Segurança).....	7
6.1.7. Responsabilização e Prestação de Contas.....	8
6.2. Padrões de Segurança	8
6.2.1. Importância da Proteção de Dados Pessoais	8
6.2.2. Garantia da Segurança dos Dados Pessoais	8
6.2.3. Obrigação do Sigilo de Dados Pessoais	8
6.2.4. Privacidade de Dados Pessoais por Concepção e por Padrão.....	8
7. DISPOSIÇÕES GERAIS.....	10

1. OBJETIVO

Esta Política tem o objetivo de estabelecer as orientações gerais para a proteção de dados pessoais dentro do ambiente corporativo da Fundação Dom Cabral (FDC) e todos os seus parceiros no Brasil e no exterior, uma vez que na execução de suas operações coleta, manuseia e armazena informações que podem estar relacionadas a pessoas físicas identificadas e/ou identificáveis (“Dados Pessoais”). Com o cumprimento das diretrizes desta política, a instituição visa a:

- Estar em conformidade com as leis e regulamentações aplicáveis de proteção de Dados Pessoais e seguir as melhores práticas;
- Proteger os direitos dos colaboradores, clientes, fornecedores e parceiros contra os riscos de violações de dados pessoais;
- Ser transparente com relação aos procedimentos da FDC no tratamento de dados pessoais;
- Promover a conscientização em toda a FDC em relação à proteção de dados pessoais e questões de privacidade.

Em particular, esta política exige que a instituição garanta que o DPO (*Data Protection Officer*) ou Encarregado de Proteção de Dados, seja consultado antes que qualquer nova atividade significativa de processamento de dados seja iniciada para garantir que as etapas de conformidade relevantes sejam tratadas.

A FDC está totalmente comprometida em garantir a implementação contínua e eficaz desta política e espera que todos os seus colaboradores compartilhem esse compromisso. Qualquer violação desta política resultar em uma ação disciplinar.

Essa política foi aprovada pelas Diretorias Estatutária e Executiva da FDC.

2. ABRANGÊNCIA

Esta Política é aplicável à **FDC** e a todos os seus **Parceiros**, tanto no Brasil quanto no exterior, e a todos os **Colaboradores** que tenham acesso a quaisquer dados pessoais detidos pela FDC ou em seu nome. Procedimentos adicionais podem ser criados de acordo com exigência da legislação local.

Qualquer legislação aplicável nas diferentes regiões nas quais a FDC atua deve prevalecer, caso esteja ou venha estar em conflito com esta Política.

3. REFERÊNCIAS

- Estatuto da FDC
- Manual de Conduta da FDC
- Carta de Convivência da FDC
- *General Data Protection Regulation ("GDPR")* na Europa
- Lei Geral de Proteção de Dados ("LGPD") no Brasil

4. DEFINIÇÕES

Para fins desta política, são considerados:

Anonimização: processo ou técnica por meio da qual os dados pessoais são tornados anônimos de tal forma que não mais se referem a uma pessoa direta ou indiretamente identificável. O anonimato deve ser irreversível. Dado anonimizado não é considerado dado pessoal.

Colaboradores: funcionários/empregados que trabalham na FDC em todos os níveis, incluindo executivos, conselheiros, diretores, estagiários e aprendizes.

Comitê de Privacidade de Dados: comitê nomeado pela Diretoria Executiva, formado por até 5 (cinco) membros, sendo, um colaborador da área do Escritório de Risco e Conformidade; um da área de Marketing; um da área da Tecnologia da Informação, um da área Jurídica e o DPO, cujas atribuições estão definidas nesta política.

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

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Dado Pessoal: qualquer informação relativa a uma pessoa singular identificada ou identificável, direta ou indiretamente, por referência a um identificador como nome, número de identificação, dados de localização, identificador on-line ou a um ou mais fatores específicos a identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa natural.

Dado Pessoal Sensível: todo dado pessoal que pode gerar qualquer tipo de discriminação e constrangimento, como por exemplo 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.

Documento Norteador: documento formal da FDC que fornece conteúdo sobre decisões, regras e orientações corporativas vitais para direcionar o trabalho na instituição com legitimidade, rastreabilidade e aplicabilidade e deve ser observado e praticado por um universo definido de colaboradores.

Encarregado de Proteção de Dados ou **Data Protection Officer (DPO):** indivíduo designado como encarregado formal de proteção de dados, conforme previsto nas leis de proteção de dados. Pode ser um colaborador ou uma pessoa terceirizada.

Gestor: todo colaborador que lidera uma equipe.

Jurídico: área responsável pela gestão dos contratos celebrados entre a FDC e terceiros.

Legítimo Interesse: o legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

- apoio e promoção de atividades do controlador; e
- proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos da Lei nº 13.709/2018.

LGPD: Lei nº 13.709/2018, da legislação brasileira, comumente conhecida como Lei Geral de Proteção de Dados Pessoais – LGPD, que regula as atividades de tratamento de dados pessoais e que também altera os artigos 7º e 16, do Marco Civil da Internet.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, que incluem, mas não se limitam a: colaboradores, professores associados e parceiros.

Pseudoanonimização: processo ou técnica por meio da qual um dado tem sua possibilidade de associação dificultada, passando a não se relacionar mais de forma direta com uma pessoa identificável (por exemplo, mencionando seu nome). O dado pseudoanonimizado continua sendo considerado dado pessoal, pois não é anônimo, sendo possível, com informações adicionais, que são mantidas separadamente, identificar a pessoa.

Tecnologia da Informação ou TI: área responsável por proteger a integridade, disponibilidade e confidencialidade dos sistemas de TI e por implementar as medidas adequadas para alcançar este objetivo. Também atua como apoio técnico do DPO.

Terceiro ou Parceiro: qualquer pessoa, física ou jurídica, que atue em nome, no interesse ou para o benefício da FDC, preste serviços ou forneça outros bens, assim como parceiros comerciais que prestem serviços à FDC, diretamente relacionados à obtenção, retenção ou facilitação de negócios, ou para a condução de

assuntos da FDC, incluindo, sem limitação, professores associados e convidados, associados regionais e outros prestadores de serviços profissionais.

Titular de Dados: pessoa natural singular identificada ou identificável a quem se refere um dado pessoal específico.

Tratamento de Dados Pessoais ou **Tratamento:** qualquer operação ou conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizado. Podem ser citados como exemplos a coleta, o registro, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

5. ATRIBUIÇÕES E RESPONSABILIDADES

5.1. Compete à Diretoria Executiva (Controladora):

- a) Por meio de ato de seu Presidente, aprovar esta Política de Privacidade e Proteção de Dados Pessoais, bem como suas alterações.
- b) Aprovar a estrutura de governança para os assuntos de privacidade e proteção de dados, inclusive a criação e composição do Comitê de Privacidade de Dados.
- c) Comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
- d) Quando exigido, elaborar relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, conforme descrito na legislação.

5.2. Compete ao Encarregado de Proteção de Dados ou *Data Protection Officer* (DPO):

- a) A implementação diária desta política.
- b) Atuar como canal de comunicação entre o controlador, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD), executando as seguintes atividades:
 - I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
 - II - receber comunicações da autoridade nacional e adotar providências;
 - III - orientar os colaboradores e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
 - IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.
- c) O DPO pode ser contatado para o exercício de suas atribuições e obtenção de maiores informações sobre esta política, se necessário, pelo e-mail: dpo@fdc.org.br.

5.3. Compete ao Comitê de Privacidade de Dados:

- a) Promover o conhecimento adequado dos principais *stakeholders* em relação à importância da proteção de dados pessoais e das atividades internas inerentes as iniciativas de privacidade.
- b) Revisar, quando necessário, as iniciativas de privacidade adotadas pela FDC, propondo melhorias para as áreas responsáveis.
- c) Discutir e tomar decisões técnicas sobre novas atividades de tratamento de dados pessoais, juntamente com as áreas proponentes das respectivas atividades.
- d) Decidir sobre as medidas técnicas a serem aplicadas para eventos de alto risco e sobre as medidas disciplinares quando necessário.
- e) Avaliar e decidir sobre incidentes de vazamento de dados pessoais, juntamente com a Diretoria Executiva.

5.4. Compete ao Escritório de Risco e Conformidade:

- a) Revisar e recomendar a aprovação desta política e suas alterações à Diretoria Executiva.
- b) Propor à Diretoria Executiva a estrutura de governança para os assuntos de privacidade e proteção de dados.
- c) Fazer o monitoramento permanente e efetivo da implementação das iniciativas de privacidade, com o objetivo de que a FDC esteja em conformidade com as leis e regulamentos relacionados à privacidade e proteção de dados pessoais, bem como com suas políticas e procedimentos internos relacionados ao tema.
- d) Implementar treinamentos, programas de conscientização e comunicação do tema de privacidade de dados pessoais para colaboradores e terceiros que atuem em processos relacionados à coleta e ao tratamento de dados pessoais.
- e) Elaborar e manter atualizados os Documentos Norteadores relativos à privacidade que estejam na sua competência.
- f) Apoiar a construção e atualização dos avisos de privacidade.
- g) Conduzir periodicamente avaliações de maturidade da FDC em relação às iniciativas de privacidade, identificando melhorias assim como a sua evolução.

5.5. Compete ao Jurídico:

- a) Assegurar que os contratos que contemplem a cessão ou o tratamento de dados pessoais conttenham cláusulas de privacidade adequadas à legislação e regulamentação aplicáveis.
- b) Prestar apoio jurídico ao DPO, ao Comitê de Privacidade de Dados e à Diretoria Executiva na ocorrência de vazamentos de dados pessoais.
- c) Prestar apoio jurídico à FDC na interpretação da legislação e regulamentação relativas à proteção de dados pessoais.
- d) Apoiar na renegociação de contratos/aditivos com fornecedores e parceiros que realizam o tratamento de dados pessoais.
- e) Apoiar o DPO na interface com Autoridades Nacionais de Dados Pessoais.

5.6. Compete à Gerência de Tecnologia da Informação:

- a) Analisar violações e vazamentos de dados pessoais bem como efetuar a coleta de evidências técnicas, compartilhando estas informações com o Comitê de Privacidade de Dados.
- b) Monitorar e implementar medidas de segurança para garantir o cumprimento da legislação e da regulamentação aplicáveis.
- c) Publicar avisos de privacidade em websites e programas externos.
- d) Revisar e manter atualizados os Documentos Norteadores relativos à segurança da informação que estejam na sua competência.
- e) Definir procedimento e *templates* para formalização de incidentes de dados pessoais.
- f) Implementar mecanismos para garantir os direitos dos titulares de dados.
- g) Prestar suporte técnico para as áreas internas e analisar novas ferramentas e sistemas com foco na exposição de dados pessoais.
- h) Garantir a aplicação das medidas de segurança tecnológica proporcionais ao risco gerado pelo tratamento de dados pessoais e em linha com a expectativa de proteção do titular do dado pessoal, garantindo a integridade, disponibilidade e confidencialidade destas informações.

5.7. Compete a todos os Colaboradores:

- a) A responsabilidade pelo tratamento adequado dos dados pessoais, devendo atuar conforme as diretrizes desta política.
- b) Antes de implementar novas atividades de tratamento de dados pessoais, levar as propostas para análise do Comitê de Privacidade de Dados.

6. DIRETRIZES

6.1. Princípios de Proteção de Dados Pessoais

Esta seção descreve os princípios que devem ser observados na coleta, manuseio, armazenamento, divulgação e tratamento de dados pessoais pela FDC para atender aos padrões de proteção de dados no âmbito corporativo e estar em conformidade com a legislação e regulamentação aplicáveis nos respectivos países onde tiver operação ou atividade educacional.

6.1.1. Legalidade, Transparência e Não Discriminação

A FDC trata os Dados Pessoais de forma justa, transparente e em conformidade com legislação e regulamentação aplicáveis.

A FDC somente trata dados pessoais quando o propósito/finalidade do tratamento se enquadra em uma das hipóteses legais permitidas, abaixo elencadas:

- a) Necessidade para a execução de um contrato do qual o titular dos dados é parte.
- b) Exigência decorrente de lei ou regulamento ao qual a FDC está sujeita.
- c) Interesse legítimo conforme definido no item 4 desta política.
- d) Necessidade de prover ao titular dos dados o exercício regular de direito em processo judicial, administrativo ou arbitral.
- e) Para realização de estudos e pesquisas, garantida, sempre que possível, a anonimização dos dados pessoais.
- f) Para fins acadêmicos, como por exemplo, registro na Secretaria Acadêmica para certificação.
- g) Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Quando o tratamento de dados pessoais não se enquadrar nas hipóteses acima, a FDC deve obter o consentimento dos titulares dos dados para o tratamento de seus dados pessoais, e assegurar que este consentimento seja obtido de forma específica, livre, inequívoca e informada. A FDC deve coletar, armazenar e gerenciar todas as respostas de consentimento de maneira organizada e acessível, para que a comprovação de consentimento possa ser fornecida quando necessário.

O consentimento também poderá ser dado pelo titular no preenchimento de formulários e fichas de inscrição no site e aplicativos da FDC ou de forma eletrônica pelo titular, ocasião em que serão explicitamente identificadas as finalidades do tratamento, que podem incluir a divulgação dos programas educacionais e institucional da FDC.

Da mesma forma, o titular de dados deve ter a possibilidade de retirar o seu consentimento a qualquer momento com a mesma facilidade que foi fornecido.

O tratamento de dados pessoais sensíveis somente é permitido nos casos específicos descritos abaixo, nos quais deverão ser observados padrões de segurança mais robustos do que os empregados aos demais dados pessoais:

- a) Quando for necessário para o cumprimento de obrigação legal ou regulatória.
- b) Quando for necessário para o exercício regular de direitos como, por exemplo, defesa ou proposição de ações judiciais ou administrativas ou arbitrais.
- c) Quando for necessário para o cumprimento de obrigações e o exercício de direitos em matéria de emprego, previdência social e proteção social.
- d) Para proteção à vida ou à incolumidade física do titular do dado incluindo dados médicos com fins preventivos, ocupacional.

- e) Para fins de promoção ou manutenção de igualdade de oportunidades entre pessoas de origem racial ou étnica diferente.
- f) Quando o titular dos dados tiver dado o seu consentimento explícito, de acordo com a legislação e regulamentação aplicáveis.
- g) Quando o tratamento for relativo a condenações penais e infrações ou a medidas de proteção relacionadas será efetuado sob o controle da autoridade pública ou quando o tratamento for autorizado pela legislação da União ou de um Estado-Membro que preveja as salvaguardas adequadas para os direitos e liberdades dos titulares de dados pessoais.

Em algumas circunstâncias, a FDC pode vir a tratar dados pessoais sensíveis, envolvendo, mas não limitado a:

- a) Dados relacionados à saúde ou à vida sexual.
- b) Dados genéticos ou biométricos vinculados a uma pessoa física.
- c) Dados sobre orientação sexual.
- d) Dados sobre condenações ou ofensas criminais.
- e) Dados referentes a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político.

6.1.2. Limitação e Adequação da Finalidade

O tratamento de dados pessoais deve ser realizado de maneira compatível com a finalidade original para a qual os dados pessoais foram coletados, não podendo ser coletados com um propósito e utilizados para outro.

6.1.3. Princípio da Necessidade (Minimização dos Dados)

A FDC somente pode tratar dados pessoais na medida em que seja necessário para atingir um propósito específico, este é o princípio da minimização de dados. O compartilhamento de dados pessoais com outra área ou outra empresa deve considerar este princípio, só podendo ser compartilhados quando tenham um amparo legal adequado.

6.1.4. Exatidão (Qualidade dos Dados)

A FDC deve adotar medidas razoáveis para assegurar que quaisquer dados pessoais em sua posse sejam mantidos precisos, atualizados em relação às finalidades para as quais foram coletados, sendo certo que deve ser possibilitado ao titular do dado pessoal a possibilidade de se requerer a exclusão ou correção de dados imprecisos ou desatualizados.

6.1.5. Retenção e Limitação do Armazenamento de Dados

A FDC deve ter conhecimento de suas atividades de tratamento, períodos de retenção estabelecidos e processos de revisão periódica, não podendo manter os dados pessoais por prazo superior ao necessário para atender as finalidades pretendidas

6.1.6. Integridade e Confidencialidade (Livre Acesso, Prevenção e Segurança)

A FDC deve assegurar que medidas técnicas e administrativas apropriadas sejam aplicadas aos dados pessoais para protegê-los contra o tratamento não autorizado ou ilegal, bem como contra a perda acidental, destruição ou danos. O tratamento de dados pessoais também deve garantir a devida confidencialidade. Dentre as medidas técnicas mais comuns, podem ser citadas a anonimização e a pseudoanonimização, conforme definidas no item 4 desta política.

6.1.7. Responsabilização e Prestação de Contas

A FDC é responsável e deve demonstrar o cumprimento desta política, assegurando a implementação de diversas medidas que incluem, mas não se limitam a:

- a) Garantia de que os titulares dos dados pessoais possam exercer os seus direitos, reconhecidos pela legislação e por esta política.
- b) Registro de dados pessoais, incluindo:
 - registros de atividades de tratamento de dados pessoais, com a descrição dos propósitos/finalidades desse tratamento, os destinatários do compartilhamento dos dados pessoais e os prazos pelos quais a FDC deve retê-los;
 - registro de incidentes de dados pessoais e violações de dados pessoais.
- c) Garantia de que os terceiros que sejam Operadores de Dados Pessoais também estejam agindo de acordo com esta política e com a legislação e regulamentação aplicáveis.
- d) Garantia de que a FDC, quando requerido, registre junto à Autoridade Nacional um Encarregado de Dados (DPO).
- e) Garantia de que a FDC esteja cumprindo todas as exigências e solicitações de qualquer autoridade de supervisão à qual esteja sujeita.

6.2. Padrões de Segurança

6.2.1. Importância da Proteção de Dados Pessoais

A FDC está comprometida com a implementação dos padrões de segurança da informação e com a proteção de dados pessoais com vistas a garantir o direito fundamental do indivíduo à autodeterminação da informação.

6.2.2. Garantia da Segurança dos Dados Pessoais

A confidencialidade, integridade e disponibilidade, bem como autenticidade, responsabilidade e não-repúdio são objetivos a serem perseguidos para a segurança dos dados pessoais.

6.2.3. Obrigação do Sigilo de Dados Pessoais

Todos os colaboradores com acesso a dados pessoais estão obrigados aos deveres de confidencialidade dos dados pessoais mediante a anuência ao Manual de Conduta e Carta de Convivência da FDC, quando do ingresso na instituição e periodicamente quando necessário.

6.2.4. Privacidade de Dados Pessoais por Concepção e por Padrão

Ao implementar novos processos, procedimentos ou sistemas que envolvam o tratamento de dados pessoais, a FDC deve adotar medidas para garantir que as regras de privacidade e proteção de dados sejam adotadas desde a fase de concepção até o lançamento/implantação destes projetos.

6.3. Relação Controlador-Operador de Dados Pessoais

Em regra, cada parceiro da FDC é o Controlador dos dados pessoais em sua respectiva organização, sendo necessária a nomeação de um responsável por garantir que os dados pessoais estejam sendo tratados de forma correta e de acordo com a legislação e regulamentação aplicáveis. Em determinadas circunstâncias, o parceiro poderá atuar como Operador da FDC ou esta pode atuar como Operadora do parceiro, sendo que, quem está atuando como Operador está obrigado a seguir a orientação de quem está atuando como Controlador.

6.4. Política de Transferência Internacional de Dados Pessoais

Quando os dados pessoais forem tratados em países diferentes de onde foram coletados, a legislação e regulamentação aplicáveis à transferência internacional de dados de cada país devem ser observadas. A FDC deve garantir a existência e atualização de contratos de transferência internacional de dados pessoais.

6.5. Direitos dos Titulares de Dados Pessoais

A FDC está comprometida com os direitos dos titulares de dados pessoais, os quais incluem:

- a) A informação, quando os dados pessoais são fornecidos, sobre como seus dados pessoais serão tratados.
- b) A informação sobre o tratamento de seus dados pessoais e o acesso aos dados pessoais que a FDC detenha sobre eles.
- c) A correção de seus dados pessoais se estiverem imprecisos, incorretos ou incompletos.
- d) A exclusão, bloqueio e/ou anonimização de seus dados pessoais em determinadas circunstâncias (“direito de ser esquecido”). Isso pode incluir, mas não se limita a, circunstâncias em que não é mais necessário que a FDC retenha seus dados pessoais para os propósitos para os quais foram coletados.
- e) A restrição do tratamento de seus dados pessoais em determinadas circunstâncias.
- f) Opor-se ao tratamento, se o tratamento for baseado em legítimo interesse.
- g) A retirar o consentimento a qualquer momento, se o tratamento dos dados pessoais se basear no consentimento do indivíduo para um propósito específico.
- h) A portabilidade dos dados pessoais a outro fornecedor de serviço ou produto, mediante requisição expressa em determinadas circunstâncias.
- i) A revisão das decisões tomadas unicamente com base em tratamento automatizado de dados pessoais;
- j) A apresentação de queixa à FDC ou à Autoridade de Proteção de Dados aplicável, se o titular dos dados pessoais tiver motivos para supor que qualquer um de seus direitos de proteção de dados pessoais tenha sido violado.

6.6. Prestadores de Serviços Terceirizados

Os prestadores de serviços terceirizados que tratem dados pessoais sob as instruções da FDC estão sujeitos às obrigações impostas aos operadores de acordo com a legislação e regulamentação de proteção de dados pessoais aplicáveis. A FDC deve assegurar que no contrato de prestação de serviço sejam contempladas as cláusulas de privacidade que exijam que o operador de dados terceirizado implemente medidas de segurança, bem como controles técnicos e administrativos apropriados para garantir a confidencialidade e segurança dos dados pessoais e especifiquem que o operador está autorizado a tratar dados pessoais apenas quando seja formalmente solicitado pela FDC.

Nos casos em que o prestador de serviços estiver localizado fora do país em que o dado pessoal foi coletado, as cláusulas contratuais padrão devem ser incluídas no contrato de proteção de dados pessoais como um anexo para garantir que as devidas salvaguardas exigidas pela legislação e regulamentação aplicáveis de proteção de dados pessoais sejam implementadas.

6.7. Gerenciamento de Violação de Dados

Todos os incidentes e potenciais violações de dados devem ser reportadas ao Encarregado de Dados (DPO). Todos os colaboradores devem estar cientes de sua responsabilidade pessoal de encaminhar e escalonar possíveis problemas, bem como de denunciar violações ou suspeitas de violações de Dados Pessoais assim que as identificarem. No momento em que um incidente ou violação real for descoberto, é essencial que os incidentes sejam informados e formalizados de forma tempestiva.

Violações de dados incluem, mas não se limitam a, qualquer perda, exclusão, roubo ou acesso não autorizado de dados pessoais controlados ou tratados pela FDC.

6.8. Auditorias de Proteção de Dados

A FDC deve garantir que existam revisões periódicas a fim de confirmar que as iniciativas de privacidade, seu sistema, medidas, processos, precauções e outras atividades incluindo o gerenciamento de proteção de dados pessoais são efetivamente implementados e mantidos e estão em conformidade com a legislação e regulamentação aplicáveis.

7. DISPOSIÇÕES GERAIS

Os colaboradores são responsáveis por conhecer e compreender todos os Documentos Norteadores que lhes forem aplicáveis. De forma similar, os gestores são responsáveis por garantir que todos os colaboradores de sua equipe compreendam e sigam os Documentos Norteadores aplicáveis à FDC.

Violações à qualquer Documento Norteador, inclusive a esta política, podem resultar em consequências graves à instituição e aos colaboradores envolvidos. Portanto, a falha em cumprir esta política ou relatar o conhecimento de violação desta política poderá resultar em medidas de responsabilização, conforme políticas internas da FDC e/ou conforme a legislação pertinente.

Os colaboradores que tiverem perguntas ou dúvidas a respeito desta política, incluindo seu escopo, termos ou obrigações, devem procurar seus respectivos gestores e, se necessário, o DPO ou o Escritório de Risco e Conformidade da FDC.

Esta política entra em vigor a partir desta data e revoga todas as disposições anteriores.

Nova Lima, 23 de agosto de 2021.



Antonio Batista da Silva Junior
Presidente Executivo

Próxima revisão: em até 2 anos a partir da data deste documento.