[ATUALIZAÇÃO 2025 DA POLÍTICA DE PRIVACIDADE E TRATAMENTO DE DADOS]

POLÍTICA DE PRIVACIDADE

POLÍTICA DE PRIVACIDADE E TRATAMENTO DE DADOS

4CO | COMUNICAÇÃO E CULTURA ORGANIZACIONAL

A presente política tem por objetivo demonstrar o comprometimento da 4CO com os procedimentos mais adequados para garantir a privacidade e proteção dos Dados Pessoais e Sensíveis, tanto em seu ambiente digital quanto analógico.

A Política de Privacidade da 4CO demonstra como coletamos, mantemos e utilizamos os DADOS nos termos da Lei Aplicável nº 13.709/2018 (“Lei Geral de Proteção de Dados Pessoais”).

A Política de Privacidade é revisada regularmente no intuito de identificar pontos que mereçam atualização ou melhorias.

Também poderá ser revisada a Política de Privacidade pontualmente a qualquer momento, à medida que surgirem atualizações (adições, alterações, correções) relevantes das atividades de tratamento de dados pessoais da 4CO e dos processos relacionados.

A Política de Privacidade será revisada imediatamente em caso de publicação de novas diretrizes por parte da Autoridade Nacional de Proteção de Dados, ou alteração em legislações que impactem

diretamente em regras de proteção de dados pessoais e que tenham impacto nos processos e atividades de gestão de direitos dos titulares de dados da 4CO.

Como condição de relacionamento profissional, comercial ou qualquer outro que seja com a 4CO, você declara que fez a leitura e ficou ciente de nossa Política.

Diretrizes e os conceitos usados pela 4CO alinhados com LGPD

Dado Pessoal

Informação relacionada à pessoa natural identificada ou identificável.

Um dado pessoal é aquela informação que, mesmo quando não identifica diretamente uma pessoa, pode ser usado para tal se combinado com outras informações.

Dado Sensível

São dados que, por sua sensibilidade, podem ser utilizados para fins discriminatórios.

Exigem, por isso, um maior cuidado no seu tratamento. São eles, portanto: os dados pessoais sobre origem racial ou étnica; sobre convicção religiosa; sobre opinião política; sobre filiação a sindicato ou à organização de caráter religioso, filosófico ou político; dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos.

Dado de Saúde

O dado de saúde é uma subcategoria prática do dado sensível.

Não é previsto como tal na lei, mas será utilizado em nossa Política para distinguir com mais precisão os dados sensíveis, referentes à saúde dos titulares, daqueles dados sensíveis mais abrangentes.

Dados de saúde incluem: diagnósticos, atuais ou pregressos, tratamentos, medicações utilizadas, hábitos, vícios, tipo sanguíneo, se é portador de doença, entre outros.

Base Legal

São os fundamentos jurídicos que autorizam a 4CO a tratar dados pessoais. Toda atividade de tratamento de dados da 4CO está pautada e fundamentada em uma base legal da LGPD, em consonância com o ordenamento jurídico brasileiro.

Titular de Dados

É a pessoa física a quem se refere os dados pessoais que são objeto de tratamento. A LGPD estabelece direitos fundamentais de liberdade e privacidade aos indivíduos em relação a seus dados, bem como regra os instrumentos administrativos e judiciais para sua proteção e garantia.

Controlador

O Controlador é a pessoa ou organização que toma decisões em relação ao modo como os dados serão tratados: a forma, a finalidade, os meios e outras diretrizes.

Operador

O operador é aquele que trata dados para o Controlador de acordo com as suas instruções, sem poder de decisão sobre a finalidade e meios gerais, mas apenas sobre detalhes técnicos e operacionais.

Tratamento

É toda operação realizada com dados pessoais. A lei demonstra o quão abrangente é o termo: 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; são formas de tratamento.

ANPD | Autoridade Nacional de Proteção de Dados

É o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados.

Colaboradores

Termo utilizado para designar todas as pessoas naturais, sejam elas clientes, colaboradores, prestadores de serviços, que se dedicam de forma direta ou indireta à execução dos objetivos da 4CO.

Encarregado | Data Protection Officer (DPO)

Pessoa responsável por fazer a intermediação entre a 4CO e a ANPD, além de ser responsável pelo programa de conformidade da organização.

A presente Política de Privacidade faz parte do arcabouço de documentos adotados pela 4CO para proteger seus colaboradores, clientes, *leads* e terceiros, no que diz respeito aos seus dados pessoais. Essa Política é o documento central do arcabouço de proteção de dados da 4CO, e, como tal, oferecerá informações gerais sobre a forma como os dados são tratados internamente.

Esses são os procedimentos e processos adotados pela 4CO e servem de referência para tratamento de dados que nossos colaboradores e clientes devem adotar para tratarmos os dados internamente e externamente. No caso de existirem documentos mais específicos sobre o tema, eles serão referenciados.

Nossa Política de Privacidade e Tratamento de Dados aborda duas frentes distintas: primeiramente, a forma como os dados pessoais deverão ser tratados dentro da 4CO, e, em segundo lugar, como os dados dos colaboradores são tratados. Além disso, apresentaremos princípios gerais que devem reger todo e qualquer uso de dados internamente.

Lembramos a todos que o tratamento de dados pessoais descreve toda e qualquer ação que envolve informação referente a uma pessoa natural, seja ela identificada direta ou indiretamente. Em caso de dúvidas ou sugestões, o colaborador deve buscar o apoio e orientação do Encarregado.

O Encarregado se responsabilizará pela garantia, manutenção e revisão da Política de Privacidade. Ele poderá utilizar de assessoria externa e/ou interna para conduzir suas atividades com eficiência.

BRUNO CARRAMENHA | SÓCIO-DIRETOR | (11) 975-478-006 | BRUNO@4CO.COM.BR

Escopo de Aplicação da Política de Privacidade

A quem a Política se aplica?

Esta Política deverá ser seguida por todos os colaboradores, terceirizados e diretores da 4CO em todos os processos envolvendo dados pessoais. Considera-se aqui como "processo envolvendo dados pessoais" toda e qualquer atividade que envolva, ainda que superficialmente (como apenas analisar ou guardar), informações relativas a pessoas físicas (mesmo que seja uma informação de contato corporativo).

Divisão de Responsabilidades

É papel de todos os colaboradores compreender essa Política e agir de acordo com suas diretrizes. Todos dentro da estrutura da 4CO devem estar preparados para receber e encaminhar devidamente solicitações de titulares de dados pessoais, assim como para alertar os responsáveis caso identifiquem possível incidente envolvendo dados pessoais.

Na 4CO, existem algumas posições que estão preparadas para lidar com situações e tomar decisões que envolvam dados pessoais. São elas:

Encarregado | Data Protection Officer (DPO)

O Encarregado é responsável por garantir a observância da LGPD em todas as atividades de tratamento de dados da 4CO. O DPO deve aconselhar a diretoria da 4CO em questões relativas à proteção de dados e à LGPD, em conjunto com a área jurídica.

O Encarregado da 4CO, no momento de elaboração desta Política, é:

Bruno Carramenha | SÓCIO-DIRETOR | (11) 975-478-006 | BRUNO@4CO.COM.BR

Segurança da Informação

A segurança da informação é uma preocupação de primeira ordem junto à proteção dos dados pessoais na 4CO. Os colaboradores devem se certificar de

que todos os dados são tratados com segurança e sigilo, tanto contra ameaças externas quanto internas. É imprescindível portanto ter ciência da Política de Segurança da Informação da 4CO, ou contatar o responsável pela segurança da informação para quaisquer dúvidas relativas ao tema.

Princípios, Direitos e Obrigações

Princípios de Proteção de Dados na LGPD

Todas as atividades dentro da 4CO que envolvem o tratamento de dados pessoais estão sempre de acordo com os princípios trazidos pela Lei Geral de Proteção de Dados. Portanto, é importante que todos conheçam esses princípios e entendam como eles interferem no dia a dia das operações da 4CO.

Os dez princípios da proteção de dados na LGPD exigem que os dados sejam:

- Tratados apenas para fins legítimos, específicos e explícitos, sem possibilidade de serem tratados de outra forma incompatível com a finalidade;
- Adequados e compatíveis com a finalidade pré-determinada;
- Limitados ao mínimo necessário para alcançar a finalidade pré-determinada;
- Facilmente consultados pelo titular (quanto a forma e duração), sem custo;
- Exatos, claros, relevantes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade;
- Tratados de forma transparente em relação ao titular de dados;
- Tratados de forma segura, utilizando medidas técnicas e administrativas apropriadas, protegidas de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração ou comunicação;
- Tratados de forma não-discriminatória, ilícitas ou abusivas;
- Tratados de forma que permita à 4CO prestar contas aos titulares, aos parceiros e às autoridades a respeito do cumprimento da lei.

Direitos dos Titulares

Segundo a Lei Geral de Proteção de Dados, os titulares têm direitos específicos com relação aos seus dados. Esses direitos podem ser requeridos frente a todos aqueles que fazem uso dessas informações, inclusive a 4CO.

Estes direitos incluem: i) direito de acesso a um documento que mostre quais dados seus estão sendo tratados, e se estão sendo tratados; ii) direito de retificação de dados que eventualmente estejam incorretos; iii) direito de exclusão, em casos específicos autorizados por lei; iv) direito de objeção ao tratamento; v) direito de portabilidade dos seus dados; vi) direito de explicação e revisão de decisões automatizadas e vii) direito de restrição do tratamento que considerar inadequado.

Estes direitos não são absolutos, e cada caso deve ser analisado pelo responsável pelo atendimento às solicitações para identificar se o titular pode exigi-lo de fato, e, em caso negativo, responder de acordo, com a devida justificativa. A resposta à solicitação deve observar os prazos e os cuidados em relação à confirmação da identidade do titular estabelecidos pela Lei Geral de Proteção de Dados.

O Encarregado da 4CO é quem endereça as solicitações ou aponta alguém que o faça.

Do papel da 4CO no tratamento de dados pessoais

Nas atividades cotidianas a 4CO atua tanto como operadora quanto como controladora dos dados, a depender do processo, e, em algumas situações, da ação a ser realizada.

Essa variação ocorre em razão da ausência de uniformidade quanto às fontes dos dados pessoais utilizados e o nível de liberdade de atuação da 4CO. Em algumas ações, as bases de dados são de nossa propriedade e controle, podendo ser reutilizada, inclusive para clientes diversos.

Nos casos em que a 4CO é a controladora dos dados pessoais, nós impomos limites aos operadores e a quaisquer terceiros que tenham acesso a essas informações. Essas medidas são adotadas através de instrumento contratual ativo entre as partes, e todas as orientações sobre o tratamento de dados pessoais são encaminhadas formalmente por canal previamente estabelecido. Em algumas situações, as atividades poderão ser realizadas diretamente por colaboradores da 4CO, utilizando-se apenas da plataforma terceirizada.

No entanto, ocorre também de a base de dados utilizada ser de propriedade do cliente, que a compartilha com um objetivo específico e restrito. Nesses casos, a 4CO é a operadora dos dados pessoais, o que impõe a obrigação de tratá-los nos limites estritos dos impostos pelo controlador (cliente), e de nenhuma forma poderão ser reutilizados para ações de outras contas.

Quando a 4CO é a operadora da base de dados, as instruções para sua atuação deverão ser recebidas formalmente, por escrito, via canal de comunicação previamente combinado com o cliente, e dentro das delimitações do contrato.

Instruções para Colaboradores

É papel de todos os colaboradores da 4CO observar integralmente as instruções apresentadas nesta Política de Privacidade, reunidas de forma detalhada e direta no Anexo III – Manual de Boas Práticas, cuja leitura e aplicação por todos é indispensável. Abaixo estão alguns exemplos de bons comportamentos que os colaboradores devem buscar em todas as suas atividades de tratamento de dados:

- Levar em conta, em todas as suas atividades cotidianas, todos os princípios e obrigações descritos nesta política.
- Restringir a coleta e o tratamento de dados ao mínimo possível. Não coletar dados “por via das dúvidas”, mas apenas quando estritamente necessário para se atingir a finalidade daquele tratamento.
- Evitar coletar e tratar dados sensíveis, como dados de saúde ou etnia. Quando inevitável, tenha cuidado redobrado e não compartilhe sem autorização do líder do projeto ou do Encarregado.
- Sempre que receber uma base de dados de fonte diversa, entre em contato com o líder do projeto ou o Encarregado para validação da origem e do atendimento aos requisitos da LGPD.
- Certifique-se, sempre que for razoável, de que os dados que você trata estão corretos e atualizados.
- Mantenha seguros os dados pelos quais é responsável: evite usar senhas fáceis e lembre-se de travar o computador quando não estiver utilizando.
- Exclua de seu computador, sempre que possível, os dados não mais necessários para atingir a finalidade da atividade de tratamento. Ex.: E-mails, arquivos baixados na área de trabalho ou pasta de “downloads” etc.

- Apenas compartilhe dados com colegas que sejam autorizados para tal, e apenas quando necessário.
- Certifique-se de que contratos com fornecedores sob sua responsabilidade contenham cláusulas de proteção de dados adequadas. Caso seja necessário fazer alguma adaptação, entre em contato com o Encarregado com a área jurídica.
- Se você for responsável pela aquisição de sistemas ou serviços de tecnologia da informação que envolvam proteção de dados, busque priorizar serviços ou sistemas que permitam a segmentação de acesso aos dados pessoais e que tenham boas garantias de proteção de dados, tais quais uma Política de Privacidade clara e concisa, sistemas seguros e serviços de atendimento ao cliente para questões envolvendo proteção de dados. Não hesite em entrar em contato via estes mecanismos para indagar a respeito das práticas de proteção de dados do fornecedor. Busque se informar sobre sub-operadores (fornecedores dos fornecedores) e onde estão localizados.
- Evite tratar dados pessoais a que se tem acesso para finalidades diversas da sua atividade profissional.
- Não colete, copie, fotografe ou capture a tela, compartilhe, disponibilize acesso para outros, ou envie informações por e-mail para pessoal não autorizado.
- Não compartilhe dados pessoais a que se tem acesso com qualquer pessoa fora da 4CO ou sem relação com o processo, a não ser que haja autorização expressa do Encarregado de dados pessoais.

Por causa da natureza de suas atividades, algumas áreas da 4CO têm obrigações específicas com relação aos dados pessoais tratados por elas. Nesse sentido, o setor de recrutamento está especialmente atento às exigências ligadas ao tratamento de dados de colaboradores e candidatos, inclusive no que diz respeito à base legal aplicável e aos prazos legais de retenção conforme determinado pela Legislação. O setor financeiro deve estar atento às regras de compartilhamento de dados pessoais com terceiros, especialmente escritórios de contabilidade e órgãos governamentais.

Tratamento de dados de colaboradores

A tabela abaixo esclarece quais dados de colaboradores são tratados por seus respectivos setores, bem como a finalidade para cada atividade de tratamento.

Setor e Atividade de Tratamento	Dados pessoais	Finalidade	Compartilhado com
Contratação	Nome, endereço, CNPJ, telefone, RG e CPF, residência, contrato social, inscrição na Prefeitura Municipal.	Contratação de colaborador	Contrato Social, cadastro de pessoa jurídica

Mais informações a respeito do tratamento de dados e com quem são compartilhados podem ser solicitados ao Encarregado pelos mecanismos de atendimento a direitos dos titulares.

Os prazos de retenção dos dados pessoais poderão ser acessados no Anexo II – Política de Retenção.

Base legal para o tratamento de dados de colaboradores

Todos os dados de colaboradores são tratados de acordo com uma das hipóteses previstas em Lei, as chamadas “bases legais”. A maior parte das atividades de tratamento de dados de colaboradores na 4CO se enquadra na hipótese de execução de contrato ou cumprimento de obrigação legal, isto é, para cumprir com obrigações previstas no contrato estabelecido ou em leis e regulamentos do setor.

Compartilhamento com terceiros

Os dados de colaboradores só são compartilhados com terceiros dentro de uma hipótese legal. A 4CO contrata fornecedores de serviços com quem compartilha dados para viabilizar a prestação do serviço.

A 4CO compartilha os dados de seus colaboradores com alguns parceiros que oferecem serviços à 4CO de pesquisa, produção de mídia, propaganda etc. Apenas são compartilhados os dados indispensáveis para o fornecimento desses serviços, e apenas quando estritamente necessário.

A 4CO é legalmente obrigada a compartilhar alguns dados com o governo, para cumprimento de obrigações legais. Os dados de colaboradores podem ser compartilhados com autoridades investigativas e regulatórias se solicitados. Neste caso, a 4CO só compartilha os dados com autoridades quando estritamente necessário, e sempre dentro dos limites da Lei.

Direitos de Titular

Como colaborador, você tem todos os direitos previstos pela Lei Geral de Proteção de Dados. Caso você deseje exercer qualquer um desses direitos, deverá entrar em contato com o Encarregado de Proteção de Dados na 4CO.

Transparência e Informação aos Titulares de Dados

Todos os documentos e políticas são revisados regularmente pelo Encarregado e pelas lideranças de setor relacionadas, para garantir que a informação neles contida esteja correta e atualizada. Caso os documentos sejam revisados ou alterados, caberá ao Encarregado e às lideranças comunicar apropriadamente aos titulares relacionados.

Em relação a candidatos e potenciais colaboradores, as informações necessárias serão providas durante o processo seletivo, e, eventualmente, em caso de solicitação.

Em relação aos terceiros, pessoa física, com quem a 4CO tenha uma relação direta, a informação será provida através de um Aviso De Privacidade. Em relação aos visitantes do site da 4CO, a informação será fornecida através do Aviso de Privacidade.

Rotinas e Diretrizes de Retenção e Exclusão

Todos os dados pessoais possuem uma previsão específica relativa ao seu apagamento. Essa informação consta na Política de Retenção de Dados da 4CO (Anexo II).

Os Registros de Operações contém informações a respeito do tempo de retenção dos dados para cada atividade de tratamento. A forma e os prazos de armazenamento e exclusão são definidos conjuntamente pelo Encarregado, pela Segurança da Informação e pela área jurídica.

Os dados pessoais na 4CO são retidos e tratados apenas enquanto dura a finalidade para as quais estão sendo tratados. Cumprida a finalidade e não havendo mais necessidade nem propósito em armazená-los, são excluídos apropriadamente, incluindo as cópias em diferentes sistemas e ativos.

Resposta a Incidentes

Um incidente de proteção de dados inclui qualquer ocorrência envolvendo o acesso ilícito a dados pessoais sob responsabilidade da 4CO. Estão incluídos vazamentos acidentais ou maliciosos, acessos não autorizados, destruição, perda, corrupção ou alteração indevida de dados pessoais, entre outros.

Caso um colaborador suspeite que um incidente de proteção de dados tenha ocorrido, deve imediatamente contatar **Bruno Carramenha** (bruno@4co.com.br) e **Fernando Augusto de Melo Franco** (fernando@melofrancoadvogados.com.br), detalhando a suspeita de incidente, contendo o máximo de informações e detalhes a respeito. É importante destacar que o colaborador não deve tentar investigar o caso por conta própria. A prioridade é se certificar de que o Encarregado recebeu e confirmou a notificação de incidente, de preferência por telefone ou presencialmente.

O Encarregado tomará as medidas apropriadas e seguirá o Plano de Resposta a Incidente da 4CO, organizando as funções de toda a equipe e das diferentes áreas na resolução do incidente.

Mais detalhes sobre como abordar uma situação de incidente, a necessidade de notificação da Agência Nacional de Proteção de Dados e a obrigação de registro dos incidentes poderão ser encontradas no Anexo I – Plano de Resposta a Incidente.

Avaliações de Risco

As avaliações de riscos são conduzidas após toda atualização do Registro das Operações de Tratamento de Dados Pessoais, ou sempre que pertinente por definição do Encarregado.

As lideranças de setor são responsáveis por garantir que os Registros de Operações em seus setores estejam sempre devidamente atualizados, notificando o Encarregado sempre que uma mudança relevante for feita.

Algumas atividades de tratamento de dados de maior risco estão sujeitas à realização de um Relatório de Impacto à Proteção de Dados (RIPD), que será conduzido antes da implementação efetiva da atividade. O RIPD determina a necessidade ou não de serem criadas medidas de mitigação dos riscos. Caso o risco da atividade ainda seja considerado muito alto após a implementação das medidas, a gestão da 4CO decidirá como proceder, juntamente com as lideranças setoriais e apoiada pelo Encarregado.

Treinamento

A fim de conscientizar a equipe a respeito de questões envolvendo proteção de dados, de introduzir uma cultura de proteção de dados na 4CO e de melhorar a segurança organizacional dos dados pessoais tratados pela 4CO, todos os colaboradores foram informados a respeito das exigências da Lei Geral de Proteção de Dados e dos documentos do Programa de Proteção de Dados desenvolvidos e adotados pela 4CO.

Rotinas de treinamento são adotadas para as diferentes funções envolvendo o tratamento de dados na 4CO.

Estes treinamentos consistem nos seguintes tópicos:

- **Introdutórios:** Um curso introdutório em Proteção de Dados é ofertado a todos os colaboradores a fim de garantir que todos estejam conscientes das regras, princípios e medidas de proteção de dados, incluindo documentos do Programa de Proteção de Dados, adotados pela 4CO.
- **Avançados:** Cursos detalhados para funções diferentes são conduzidos regularmente, abordando questões específicas de acordo com a função.

Os treinamentos avançados são realizados anualmente com todos os colaboradores de acordo com a necessidade.

Atualização dos Documentos do Programa de Proteção de Dados e dos Registros das Operações de Tratamento

Os documentos do Programa de Proteção de Dados da 4CO, incluindo os Registros das Operações de Tratamento, são revisados regularmente a fim de garantir que estejam sempre corretos e atualizados. Os prazos específicos são definidos pelo Encarregado.

Etapas de tratamento de dados na 4CO

Cuidados em todas as fases do projeto

Ao executar qualquer etapa do projeto, os colaboradores e parceiros da 4CO devem sempre ter em mente os princípios da Lei Geral de Proteção de Dados. A coleta e o tratamento de dados devem ser limitados a sua finalidade, de modo que dados que não possuem ligação com o objeto e a finalidade do projeto não devem ser coletados.

O Anexo III - Manual de Boas Práticas no Tratamento de Dados deve ser utilizado como base para todo o tratamento dos dados, desde o início do projeto até a exclusão definitiva dos dados, a fim de se evitar armazenamento e envio de dados por meios inadequados ou vulneráveis, especialmente quando se tratar de dados pessoais coletados e tratados pela 4CO. Em todas as etapas o líder do projeto deve anotar as alterações relevantes no Registro de Operações com Dados para a adequada fiscalização e controle por parte do Encarregado.

Registro de Operações de Tratamento de Dados Pessoais

As atividades de tratamento de dados serão documentadas nos registros de operação de tratamento de dados pessoais. Os registros contêm informações das categorias e tipos de dados pessoais tratados, as finalidades do tratamento e outras informações relativas a terceiros envolvidos nas atividades de tratamento.

Os registros devem ser revisados e atualizados regularmente, de forma que a informação contida neles esteja sempre atualizada. A organização desses registros deve se dar da seguinte forma:

i. **Registro de Operações com Dados.** Todo líder de projeto deve organizar seu Registro de Operações, com todos os detalhes a respeito dos dados que o projeto utilizará, como o tipo de dados, onde serão armazenados, a data de início e de encerramento do tratamento, o tipo de tratamento e eventualmente a confirmação da exclusão dos dados. O Registro de Operações deve ser disponibilizado ao Encarregado para fiscalização e controle toda vez que for alterado.

ii. **Registros de Atividades de Tratamento de Dados.** O Encarregado deverá reunir em um mesmo local ou documento todos os Registros de Operações com Dados, além

dos detalhes de tratamento de dados dos colaboradores da 4CO. Esse “Registros de Atividades de Tratamento de Dados” será o principal instrumento de controle do Encarregado de tudo relacionado a dados pessoais sob responsabilidade da 4CO.

O Encarregado será responsável por manter os Registros de Atividades de Tratamento de Dados atualizados. Apenas o Encarregado e a diretoria da 4CO terão permissão para editar os registros.

As lideranças de setor deverão sempre cooperar com o Encarregado para aperfeiçoar os registros, e devem sempre informá-lo caso haja uma mudança nos processos de seu setor, a fim de que os Registros possam ser atualizados. Deverão também informar o Encarregado sobre a contratação de novos fornecedores e sistemas que envolvam o tratamento de dados pessoais, para que possam ser feitas devidas avaliações de risco.

Etapa 1: Início do projeto

Neste momento, após as reuniões iniciais de alinhamento, a 4CO recebe informações compartilhadas pelo cliente que poderão envolver dados pessoais de seus colaboradores, como documentos de identificação, remuneração, dados de contato, histórico profissional, entre outras informações, inclusive dados sensíveis.

Ao iniciar o tratamento da documentação inicial, deve-se sempre filtrar os dados que não são necessários para execução do projeto. Do mesmo modo, o envio do questionário para pesquisa quantitativa deverá utilizar os dados de contato fornecidos pelo cliente.

Para iniciar a execução do projeto o líder deverá definir o escopo do tratamento de dados do projeto, como estes dados serão armazenados, o tipo de tratamento e demais condutas definidas no Registro de Operações com Dados. Este documento servirá como guia para orientar a equipe acerca do adequado tratamento de dados considerando a especificidade do projeto.

O Registro de Operações com Dados e todas as suas alterações deve ser disponibilizado ao Encarregado, por se tratar do principal instrumento de fiscalização e controle do tratamento de dados do projeto.

Etapa 2: Pesquisa e análise quantitativa

A pesquisa e análise quantitativa demanda cuidados adicionais, vez que a coleta dos dados envolve plataformas de terceiros que hospedam formulários de pesquisa a serem preenchidos. As informações compartilhadas por colaboradores do cliente, por exemplo, são a base para a realização da análise quantitativa.

É fundamental que o formulário contenha aviso de tratamento de dados, com descrição da finalidade do tratamento e a possibilidade de compartilhamento com terceiros para atingir a finalidade pretendida, bem como a possibilidade de revogação do consentimento.

Cabe ao líder do projeto determinar quais perguntas irão compor o questionário, para que o tratamento de dados seja alinhado de acordo com a finalidade estabelecida no escopo do projeto.

Após a extração do relatório da plataforma de pesquisa, os dados devem ser armazenados nos servidores, e, após, geralmente são enviados para parceiros que irão refinar o relatório extraído, por meio de seleção e formatação das planilhas para análise da 4CO. Por essa razão, há necessidade do respeito às boas práticas, vez que os dados serão tratados por um terceiro alheio à 4CO.

O compartilhamento de dados somente poderá ocorrer com terceiros que tenham relação contratual com a 4CO com disposições acerca do tratamento de dados e os limites da responsabilidade pelo tratamento de dados. Assim o compartilhamento dos dados com terceiros deverá ser feito pelos canais apropriados para evitar incidentes de segurança.

Etapa 3: Pesquisa e análise qualitativa

A pesquisa qualitativa, por sua vez, envolve entrevistas com colaboradores do cliente, as quais podem ser realizadas de maneira presencial ou virtual. Essas entrevistas utilizam geralmente um roteiro de perguntas que resulta em coleta de dados pessoais, inclusive dados sensíveis, como etnia, religião, saúde etc, além de relatos sigilosos a respeito de experiências profissionais, de modo que o tratamento destes dados deve ser tratado com muito cuidado.

Neste ponto os colaboradores da 4CO deverão sempre se ater ao questionário, evitando a coleta de dados que não estejam dentro da finalidade do projeto.

Ao coletar e tratar esses dados, será necessário o cuidado para que arquivos físicos sejam, sempre que possível, transformados em arquivos digitais e armazenados nos diretórios da 4CO, evitando o armazenamento nos dispositivos pessoais do entrevistador.

O armazenamento deverá observar todas as preocupações relativas à guarda e classificação dos dados coletados, especialmente quanto a anonimização dos dados sempre que possível.

Etapa 4: Análise dos dados coletados

Após a coleta, refinamento e armazenamento de todos os dados coletados, seja pela pesquisa quantitativa ou qualitativa, a 4CO passará à análise desses dados e à elaboração de diagnóstico para apresentação ao cliente. Sempre que possível, os dados a serem integrados aos relatórios e pareceres para apresentação ao cliente devem ser anonimizados, sem exposição desnecessária ou individualizada.

Caso o projeto tenha etapas de implementação pós-diagnóstico em que haja tratamento de dados pessoais, todos os cuidados utilizados anteriormente devem ser mantidos. Ações realizadas junto ao cliente como reuniões com colaboradores ou treinamento de líderes devem ser realizadas observando os procedimentos de tratamento de dados e evitando a exposição desnecessária ou individualizada.

Etapa 5: Encerramento de tratamento de dados

O encerramento do tratamento de dados geralmente ocorre quando a finalidade da coleta dos dados foi alcançada ou quando os dados não são mais necessários para essa finalidade. O tratamento também pode ser encerrado pela revogação do consentimento do titular dos dados, pelo fim contratual do período de tratamento ou por determinação da Autoridade Nacional de Proteção de Dados.

Deste modo, a depender do serviço, o fim do tratamento de dados pela 4CO ocorrerá quando os dados não forem mais necessários para o andamento do projeto ou quando ocorrer a finalização definitiva da prestação dos serviços ao cliente. A decisão de encerramento do tratamento deve ser tomada pelo líder do projeto conjuntamente com o Encarregado.

Armazenamento e exclusão

Quando determinado o encerramento do tratamento de dados, a 4CO procederá com a exclusão de todos os dados pessoais utilizados para a execução do projeto que estejam em sua posse, o que inclui pastas, diretórios, servidores, e-mails, apps de mensagem, bem como arquivos em computadores e em dispositivos móveis, entre outros. É responsabilidade do líder orientar todos os colaboradores do projeto pela exclusão de todos os dados.

A exclusão dos dados somente não ocorrerá por determinação contratual, por hipótese de retenção nos termos do Anexo II ou por necessidade de transferência do banco de dados ao cliente previamente à exclusão.

Após a exclusão de todos os dados tratados, deve ser enviada notificação ao cliente acerca da exclusão de todos os dados tratados. Por fim o envio da notificação deverá ser anotado no Registro de Operações com dados com o devido arquivamento do comprovante de envio da notificação.

ANEXO I – PLANO DE RESPOSTA A INCIDENTE

Introdução

Este Plano de Resposta a Incidentes de Segurança da Informação Envolvendo Dados Pessoais (“Plano de Resposta a Incidente” ou “PRI”) estabelece o procedimento para a gestão de situações após a identificação da ocorrência, ou mera suspeita, de um incidente de segurança da informação que envolva dados de pessoas naturais identificadas ou identificáveis que são tratados pela 4CO, visando o combate dos riscos e a minimização de eventuais efeitos relacionados a incidentes desta natureza.

O presente PRI foi elaborado de acordo com a Lei 13.709/18 (“Lei Geral de Proteção de Dados Pessoais”).

Objetivo

Este PRI tem como objetivo estabelecer as funções e responsabilidades das equipes da 4CO, bem como as medidas a serem tomadas por essas equipes para que a 4CO responda adequadamente a um incidente, sempre prezando pela integridade dos sistemas, proteção de todas e quaisquer informações que possam viabilizar, direta ou indiretamente, a identificação de uma pessoa física e a privacidade dos seus titulares, possibilitando à 4CO manter a confiabilidade de suas marcas e serviços. Também estão compreendidas dentro do conceito de dados pessoais todas as informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, informações referentes à saúde ou à vida sexual, dados genéticos ou biométricos e quaisquer dados que, quando tratados de forma combinada com outras informações, possam permitir inferir informações dessa natureza.

Este PRI se aplica em qualquer caso de incidentes envolvendo dados pessoais e deverá ser executado, em conjunto com as demais políticas da 4CO, por todas as áreas e colaboradores da 4CO, incluindo, sem limitação, os sócios, diretores, administradores, empregados e determinados prestadores de serviços e parceiros (“colaboradores”) que, no âmbito das suas relações com a 4CO, possam vir a ter acesso às áreas, equipamentos, informações, redes e aos arquivos e dados sob controle da 4CO.

O que é um incidente de segurança da informação envolvendo dados pessoais?

Para fins deste plano, entende-se por “incidente” toda e qualquer violação de segurança que, de forma acidental ou dolosa, enseje ou seja capaz de dar ensejo à destruição, perda, alteração, divulgação ou ao uso ou acesso não autorizado a dados pessoais tratados pela 4CO.

Um incidente pode ocorrer de forma maliciosa, ser o resultado de um erro humano ou, até mesmo, de falha nos sistemas que processam dados pessoais ou nos seus mecanismos de segurança.

Isso pode incluir, por exemplo, o furto de um documento, o envio de um e-mail contendo dados pessoais para destinatários indesejados, tentativas de invasão a sistemas da 4CO ou outras ações, culposas ou dolosas.

Os incidentes podem ser de vários tipos, como por exemplo:

i. **Vazamento de Dados Pessoais.** É o incidente no qual dados pessoais são indevidamente expostos e disponibilizados, por meios físicos ou digitais, para um número indeterminado de pessoas, no Brasil ou em qualquer país;

ii. **Negação de Serviço.** É o incidente no qual o acesso (lógico ou físico) a um sistema que armazene dados pessoais é prejudicado ou impossibilitado, de forma que a integridade dos dados pessoais (existência e/ou veracidade) pode ser comprometida permanentemente, dada a indisponibilidade do acesso;

iii. **Acesso Não Autorizado.** É o incidente no qual o acesso (lógico ou físico) a um sistema que possua dados pessoais é tentado ou obtido, sem que se tenha a devida autorização para tal acesso. Considera-se acesso não autorizado qualquer acesso cuja permissão para conexão, leitura, gravação, autenticação, modificação, eliminação ou criação não tenha sido concedida; e

iv. **Uso Inapropriado.** É o incidente no qual há a violação das políticas de uso de dados, informações e sistemas da 4CO.

Papéis e Responsabilidades

Todos na 4CO tem responsabilidades quando da ocorrência ou mera suspeita de um incidente, conforme descrito a seguir:

Obrigações de Todas as Áreas

i. comunicar imediatamente ao Encarregado (conforme descrito abaixo), sobre a ocorrência ou a mera suspeita de um incidente;

ii. cumprir rigorosamente a Política de Segurança da Informação da 4CO, contribuindo para a mitigação de riscos; e participar de treinamentos e programas de conscientização para mitigação de Incidentes.

Obrigações do Encarregado (DPO)

O Encarregado – **Bruno Carramenha, sócio-diretor** – é a pessoa designada para atuar em tudo o que diz respeito à proteção de dados na 4CO, incluindo nas respostas a incidentes**.** Entre suas principais responsabilidades durante o PRI, destaca-se:

i. atuar para detectar e corrigir os incidentes;

ii. realizar a triagem de risco do incidente e determinar o plano de resposta correspondente;

iii. alertar, comunicar e aconselhar os colaboradores sobre incidentes emergentes;

iv. educar e conscientizar os colaboradores sobre a detecção e resposta aos incidentes; e

v. adotar demais medidas para prevenir incidentes e minimizar o impacto de seus efeitos.

Obrigações de Outras Áreas

A equipe de resposta e o Encarregado deverão acionar outros colaboradores de outras áreas, dependendo do tipo e da gravidade do incidente.

Neste caso, segue abaixo lista de áreas que podem ser envolvidas e suas responsabilidades:

iii. **Área Jurídica.** A equipe jurídica da 4CO deverá ser consultada sempre que houver risco de responsabilização da empresa em um incidente de segurança. Responde diretamente à diretoria;

iv. **Segurança da Informação.** Auxilia na resolução das questões técnicas relacionadas ao incidente e na investigação da origem e das razões para ocorrência do incidente;

v. **Desenvolvimento.** Considerando a *expertise* do setor, deverá prestar auxílio em caso de incidente que envolva quaisquer meios digitais, além de apoiar na criação de uma ponte de comunicação com o time de segurança da informação.

Detecção do Incidente

Detectar incidente de forma rápida e eficiente é essencial para resolução bem-sucedida. São várias as formas de detecção, de modo que é impossível desenvolver uma metodologia que contemple cada uma. Desta forma, **todos os colaboradores** devem atentar-se, principalmente, aos sinais mais comuns que podem desencadear um incidente, como invasões de rede, perda ou furto de documentos ou dispositivos, *phishing*, *malware*, instabilidades sistêmicas etc.

Uma vez detectado um incidente ou suspeita de incidente, o colaborador deverá comunicar imediatamente o Encarregado, Bruno Carramenha, além do representante da área jurídica, Fernando Augusto de Melo Franco, nos contatos abaixo:

BRUNO CARRAMENHA | ENCARREGADO E SÓCIO-DIRETOR

(11) 975-478-006 | BRUNO@4CO.COM.BR

FERNANDO MELO FRANCO | ÁREA JURÍDICA

(11) 971-492-217 | FERNANDO@MELOFRANCOADVOGADOS.COM.BR

É importante que o colaborador realize a comunicação de suspeita de incidente o mais rápido possível, bem como notifique imediatamente todos os colegas de projeto do ocorrido. Na medida do possível, essa comunicação deverá conter (i) a hora e a data em que a suspeita do incidente foi descoberta; (ii) o tipo de informações envolvidas; (iii) a causa e a extensão do incidente; (iv) o contexto do ocorrido; bem como (v) qualquer informação adicional que sirva para facilitar o entendimento do evento, suas causas e consequências.

A COMUNICAÇÃO SOBRE A SUSPEITA DE UM INCIDENTE É VITAL PARA A 4CO. ASSIM, CASO O COLABORADOR SUSPEITE DE UM INCIDENTE E NÃO O COMUNIQUE, SANÇÕES DISCIPLINARES E/OU JURÍDICAS PODERÃO OCORRER, A DEPENDER DA GRAVIDADE DO INCIDENTE E DA COMPROVAÇÃO DE EVENTUAL NEGLIGÊNCIA DO COLABORADOR.

Priorização e Triagem de Risco

Uma vez que o incidente foi identificado e classificado, é necessário priorizá-lo conforme o nível de risco oferecido à 4CO e aos titulares dos dados pessoais eventualmente afetados e a gravidade da ocorrência. O impacto deve ser aferido da seguinte forma:

Volume de Dados Pessoais expostos	Baixa	Média	Alta
Alto	**Alta Gravidade**	**Alta Gravidade**	**Alta Gravidade**
Médio	**Média Gravidade**	**Alta Gravidade**	**Alta Gravidade**
Baixo	**Baixa Gravidade**	**Média Gravidade**	**Média Gravidade**

Sensibilidade dos Dados Pessoais afetados

VOLUME DE DADOS PESSOAIS EXPOSTOS	
Criticidade	**Descrição**
Alto	Volume de dados pessoais afetado superior a 10% da base de dados controlada pela 4CO
Médio	Volume de dados pessoais afetado inferior a 10% e superior a 2% da base de dados controlada pela 4CO
Baixo	Volume de dados pessoais afetado inferior a 2% da base de dados controlada pela 4CO

SENSIBILIDADE DOS DADOS PESSOAIS AFETADOS	
Criticidade	**Descrição**
Alta	Dados pessoais de crianças ou adolescentes, dados pessoais sensíveis ou que possam gerar discriminação ao titular; dados bancários, de pagamento ou de proteção ao crédito
Média	Dados pessoais imediatamente identificáveis (p.ex. nome, e-mail, CPF) combinados ou não com informações comportamentais (p.ex. histórico de atividades, preferências etc.)
Baixa	Dados anonimizados, dados pessoais pseudonimizados (desde que a chave de desanonimização também não tenha sido comprometida), dados pessoais de difícil identificação (p.ex. IP)

Procedimentos para Resposta

De acordo com a matriz acima definida, o Encarregado, em conjunto com a área de Segurança da Informação e as lideranças de setores, deverá coordenar as seguintes ações do Plano de Resposta a Incidente, simultaneamente ou, quando não for possível, em rápida sucessão:

Baixa Gravidade

i. **Priorizar a resolução do incidente.** Assim que notificado sobre a suspeita de incidente de segurança, o Encarregado deve trabalhar prioritariamente para sua resolução.

ii. **Realizar a Triagem de Risco**. Após tomar conhecimento da extensão do incidente, o Encarregado deve classificar o ocorrido de acordo com sua gravidade (baixa, média ou alta), com base nas instruções deste Anexo I. A classificação de risco deve ser informada assim que possível à direção da 4CO e à área jurídica.

iii. **Minimizar os efeitos causados como Controlador ou Operador**. No primeiro momento, a prioridade é promover o fim da vulnerabilidade de dados e mitigar os danos aos titulares e à 4CO. Isso pode significar medidas técnicas, como retirar conteúdo do ar ou bloquear acesso a servidores, ou comunicativas, como notificar partes envolvidas. A natureza do serviço prestado pela 4CO, neste caso, será determinante:

> se a 4CO for Controladora dos dados, deve seguir à risca seu Plano de Resposta;

> se for Operadora, deve se comunicar com o Controlador (cliente) e seguir seus ditames na resolução do incidente, em consonância com a Política de Privacidade e com o Plano de Resposta.

iv. **Acionar a área de Segurança da Informação**. Se necessário, o Encarregado deve contatar imediatamente os responsáveis pela Segurança da Informação.

v. **Comunicar e organizar áreas envolvidas**. O Encarregado, apoiado pelas lideranças dos setores, deve comunicar as áreas atingidas a respeito do incidente e da implementação imediata do PRI. As equipes devem ser orientadas a priorizar a solução do incidente e a obedecer a hierarquia de comando para solucionar a crise.

vi. **Documentar o incidente**. Sempre que possível, todas as etapas do PRI devem ser devidamente documentadas, por meio de relatórios, documentos, mensagens, *prints*, enfim, por todas as formas legalmente possíveis, com riqueza de detalhes.

vii. **Comunicar o ocorrido à área jurídica**. Caso ainda não tenha sido contatada, a área jurídica deve ser chamada para auxiliar na análise de risco e avaliação das consequências jurídicas do incidente.

viii. **Notificação formal à ANPD e/ou aos Titulares dos Dados**. A notificação da Autoridade Nacional de Proteção de Dados e dos titulares dos dados pessoais a respeito do incidente pode ser uma obrigação legal a ser cumprida pela 4CO a depender do caso. A decisão a respeito de qualquer notificação neste sentido é do Encarregado, após consulta à área jurídica.

ix. **Análise do incidente e medidas de prevenção**. Após a resolução do incidente, o Encarregado deve promover uma análise conjunta com todas as áreas pertinentes para analisar o incidente e antecipar, prevenir e melhor identificar incidentes semelhantes no futuro. De preferência, essas reuniões e conclusões devem ser transcritas em ata, que deverá ser apresentada à direção da 4CO e transformada em medidas concretas pelo Encarregado.

Média Gravidade

i. **Adotar todas as medidas previstas no PRI de baixa gravidade**. O Plano de Resposta para incidentes de média gravidade deve seguir todas as etapas descritas no PRI de baixa gravidade, na ordem descrita.

ii. **Realizar treinamento imediato interno com colaboradores**. Assim que possível, reunir as áreas afetadas para conscientizar os colaboradores sobre o incidente e as medidas preventivas urgentes para evitar novos problemas.

iii. **Acionar área jurídica imediatamente**. No caso de incidente de média gravidade, o suporte jurídico se torna ainda mais prioritário, devendo ser acionada o quanto antes.

Alta Gravidade

i. **Adotar todas as medidas previstas no PRI de baixa e média gravidade**. O Plano de Resposta para incidentes de alta gravidade deve seguir todas as etapas descritas no PRI de baixa e média gravidade, na ordem descrita.

ii. **Reunião emergencial entre Encarregado, sócios, líderes e área jurídica**. No caso de o volume de dados pessoais afetado ser superior a 10% da base de dados controlada pela 4CO, o Encarregado deve, assim que possível, convocar reunião com os demais sócios, líderes de setores e área jurídica para gerenciamento de crise, com definição de prioridades imediatas.

iii. **Comunicar e aplicar medidas emergenciais a todos os colaboradores**. Após a reunião emergencial, comunicar a todos os colaboradores da 4CO as medidas urgentes de gerenciamento de crise e prevenção, bem como garantir a aplicação destas. Recomenda-se, novamente, registrar e documentar hora a hora todas as medidas de resolução tomadas pela empresa, especialmente durante incidente de alta gravidade.

Comunicação do Incidente

Em cumprimento à legislação brasileira, incidentes considerados relevantes são comunicados à Autoridade Nacional de Proteção de Dados (ANPD), preferencialmente dentro de 72 horas. A avaliação sobre quais incidentes são materialmente relevantes será feita pelo Encarregado, em conjunto com a diretoria da 4CO e com a área jurídica.

Caso um incidente seja identificado como relevante e a sua comunicação à ANPD seja determinada, o Encarregado deve organizar, junto a área jurídica, a documentação aplicável à comunicação, contendo:

i. a descrição da natureza e da categoria dos dados pessoais afetados (ex. dados sensíveis, dados de criança, dados cadastrais etc.);

ii. as informações sobre os titulares dos dados pessoais envolvidos, a relação dos titulares dos dados pessoais afetados com a 4CO, o número de titulares afetados e o país de residência dos titulares dos dados pessoais afetados;

iii. a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, observados os segredos comercial e industrial;

iv. os riscos relacionados ao incidente;

v. os motivos da demora, no caso de a comunicação não ter sido feita de forma imediata;

vi. as medidas que foram e as que serão adotadas para reverter ou mitigar os efeitos do incidente.

Caso seja decidido a comunicação sobre o incidente aos titulares dos dados pessoais afetados, será desenvolvida comunicação, priorizando (i) os fatos ocorridos; (ii) as medidas tomadas pela 4CO para minimizar o impacto dos efeitos; (iii) as eventuais medidas que possam ser tomadas pelos próprios titulares dos dados pessoais afetados para mitigar riscos; e (iv) os canais de contato para sanar dúvidas.

Em caso de dúvidas, comentários e/ou sugestões deste PRI, entre em contato com o Encarregado da 4CO, que está à disposição nos seguintes endereços de contato:

BRUNO CARRAMENHA | SÓCIO-DIRETOR | (11) 975-478-006 | BRUNO@4CO.COM.BR

ANEXO II – POLÍTICA DE RETENÇÃO

Introdução

Segundo a Lei Geral de Proteção de Dados, sempre que um dado pessoal é tratado, é necessário que haja um prazo de retenção para essa informação, ou seja, um prazo depois do qual ela será excluída definitivamente. Dessa forma, há uma garantia mais acertada de que os dados não serão utilizados de maneira incompatível com a finalidade original da coleta, além de ser também uma forma de proteção da 4CO, já que danos de um eventual vazamento serão menores.

Momento da exclusão dos dados tratados

O prazo de retenção está intrinsecamente ligado à finalidade da coleta do dado. Em seu artigo 15, a Lei Geral de Proteção de Dados traz como a primeira hipótese de término do tratamento a verificação do cumprimento da finalidade para o qual o dado foi coletado, ou seja, já se atingiu o objetivo originalmente buscado. Dessa forma, o ideal é que a destruição do dado seja feita imediatamente ao se constatar que a finalidade foi cumprida.

Outras hipóteses que a Lei prevê para o fim do tratamento de dados pessoais é quando se encerra o prazo previsto para aquela atividade, a comunicação do titular, no exercício de seus direitos, ou a determinação da Autoridade Nacional de Proteção de Dados, nos termos descritos na LGPD.

O término do tratamento de dados implica na imediata destruição das informações e de todas as suas cópias, seja em meio físico ou digital.

Se os dados se encontram em papel, é importante que seu descarte seja feito através da destruição do meio no qual eles estão inseridos.

Classificação interna do banco de dados

Operacionais: Registros utilizados no dia a dia do trabalho das equipes 4CO.

Recrutamento: Dados de colaboradores da 4CO, coletados para permitir a contratação, o cumprimento de obrigações legais de contratante, a entrega de contrapartida ao contratado, entre outros.

Segurança: Dados coletados para gerenciamento de acesso às instalações da 4CO e aos sistemas utilizados pela 4CO.

Negócios: Informações relativas à condução de negócios da 4CO, incluindo fechamento de contratos, contatos comerciais, e prospecção.

Cada tipo de registro possui prazos específicos para descarte, o que equivale ao seu prazo de retenção. Todos os dados pessoais armazenados pela 4CO possuem previsão de descarte, seja pelo decurso do tempo ou pelo exaurimento da finalidade para a qual foram coletados.

Em algumas situações, existirão previsões legais que determinarão o prazo de retenção das informações, como em caso de dados tributários e trabalhistas. Nesse caso, a 4CO se reserva o direito de alterar os prazos previstos nesta política de acordo com as exigências legais.

Tipo de registro	Descrição	Retenção	Descarte
Prestadores de Serviço	Admissão (nome, RG, CPF, data de nascimento, endereço, escolaridade, e-mail, telefone, CNPJ	2 anos	2 anos
Clientes e Parceiros	Contratos (qualificação dos sócios no contrato social)	2 anos após rescisão	2 anos após rescisão
Colaboradores de Clientes	Dados Pessoais coletados para a execução de projetos	Não há	Após alcance da finalidade do tratamento

Rotina de destruição

Uma vez que o prazo determinado seja atingido, a 4CO fará a eliminação dos documentos contendo dados pessoais. Caso existam cópias armazenadas em meio físico, elas serão destruídas como resíduo confidencial, enquanto cópias digitais serão apagadas de maneira definitiva dos sistemas da 4CO e de seus fornecedores e parceiros.

Caso exista um motivo válido para a manutenção dos registros, como a existência de investigações ou processos administrativos ou judiciais, esses dados poderão ser mantidos além do período previsto, ainda que sem o consentimento do titular.

Em relação ao alcance da finalidade ao tratamento de dados necessários para execução de projetos, caberá ao líder do projeto em conjunto com o Encarregado decidir o momento em que houve o encerramento do tratamento de dados. Assim, decidido que a finalidade foi alcançada, o líder deverá

orientar e cobrar de todos os colaboradores do projeto a exclusão de todos os dados.

Após a exclusão dos dados, o registro da exclusão deverá ser anotado no Registro de Operações com Dados para arquivamento e controle em caso de necessidade futura.

Em caso de dúvidas sobre esta Política, o Encarregado deve ser contatado:

BRUNO CARRAMENHA | SÓCIO-DIRETOR | (11) 975-478-006 | BRUNO@4CO.COM.BR

ANEXO III – MANUAL DE BOAS PRÁTICAS NO TRATAMENTO DE DADOS

Introdução

Este Manual de Boas Práticas no Tratamento de Dados foi pensado para orientar os colaboradores da 4CO a como lidar com informações, arquivos, imagens, documentos, enfim, todos os dados pessoais em qualquer formato, sensíveis ou não, no cotidiano da empresa e na comunicação com clientes e colegas.

Atualmente, grande parte dos serviços prestados no Brasil e no mundo em alguma medida envolve dados pessoais. No atual contexto mundial, cada vez mais conectado e em rede, trabalhar com produtos, serviços e marcas significa inegavelmente coletar, armazenar e analisar informações. Em outras palavras, tratamento de dados.

Esse incremento de complexidade socioeconômica se traduziu nos últimos anos no Brasil na consolidação de leis que buscam regrar a coleta e manipulação de dados de pessoas, bem como garantir direito à privacidade, liberdade e dignidade da pessoa humana. A Lei 13.709/18 (“Lei Geral de Proteção de Dados Pessoais”), é o maior exemplo nacional de tentativa de regulação do uso e exploração de dados digitais na sociedade.

Além disso, há mais uma peculiaridade da “era digital”: o trabalho, hoje, ocupa cada vez mais nossos espaços pessoais, seja no ato de trabalhar em regimes híbridos (a residência como extensão do espaço de trabalho), seja nos instrumentos de trabalho, cada vez mais misturados a nossas ferramentas pessoais (smartphones, notebooks e aplicativos de mensagens como extensão da vida profissional).

A consequência dessa realidade, no contexto da 4CO, é que o tratamento de dados toma uma escala muito além dos limites físicos da agência. O comportamento de cada colaborador e seus respectivos equipamentos eletrônicos compõem o “ecossistema” de tratamento de dados.

Por essa razão, as boas práticas no que se refere a manipulação de dados pessoais devem ser seguidas por todos na 4CO, desde colaboradores até líderes de setores e sócios-diretores. Apenas com a contribuição de todos será possível atuar de forma livre, criativa e segura na missão da agência de ofertar serviços de excelência a seus clientes e, sobretudo, fiel aos princípios internos de respeito e trabalho humanizado.

O presente Manual de Boas Práticas foi elaborado de acordo com a Lei 13.709/18 (LGPD), em consonância com a Constituição Federal de 1988 e com a legislação brasileira.

Responsabilidade Compartilhada

Primeiramente, toda a equipe da 4CO deve observar que as boas práticas no tratamento de dados representa, na verdade, um compartilhamento de responsabilidades. A Política de Privacidade e de Tratamento de Dados foi desenvolvida com o intuito de adaptar o cotidiano da agência às obrigações legais da atualidade. Nesse contexto, na eventualidade de um incidente de segurança, ou seja, uma vulnerabilização de dados pessoais sob responsabilidade da 4CO, as práticas e atos de cada aspecto do tratamento de dados será analisada, tanto internamente quanto externamente. Isso significa que a estrutura de segurança da informação, os protocolos internos e o treinamento dos colaboradores se tornam igualmente importantes para evitar incidentes de segurança e danos a titulares de dados e clientes. Sendo assim, a melhor forma de se compreender as regras internas de tratamento de dados é o de responsabilidade compartilhada, na qual a agência e seus prestadores de serviços devem fazer cada qual sua parte para que não ocorram incidentes.

Respeito ao Treinamento e à Política de Privacidade são obrigatórios

Como já exposto ao longo da Política de Privacidade, a 4CO realizará treinamentos periódicos com toda a equipe a respeito de tratamento de dados. Além das reuniões, integra o treinamento dos colaboradores a leitura da Política de Privacidade e seus anexos, incluindo este Anexo III – Manual de Boas Práticas. É obrigatório a todos o respeito às instruções apresentadas, seja na forma documental, seja nas sessões de treinamentos. Caberá aos líderes de projetos e setores se certificarem que a prestação de serviços dos colaboradores ocorra em respeito estrito à LGPD e às diretrizes da 4CO.

Manual de Boas Práticas - Colaboradores

Condutas gerais

Todos os colaboradores da 4CO observar integralmente as instruções apresentadas neste Manual de Boas Práticas, sendo sua leitura e aplicação obrigatória. Parte significativa da atuação da agência em seus projetos implica na coleta e análise de dados, portanto, as seguintes condutas devem sempre estar em ação na prestação de serviço à 4CO e aos clientes, seja em ambiente físico ou digital:

- A primeira regra, acima de tudo, é considerar que toda e qualquer informação dos clientes da 4CO, em especial as que dizem respeito a funcionários e a cultura organizacional, deve ser interpretada como "**DADO**" e, consequentemente, deve sempre receber grande cuidado no seu manuseio, desde o recebimento até a exclusão definitiva.

- Privacidade desde a concepção e por padrão (Privacy by Design e by Default). Priorizar sempre, em todas as condutas, a

segurança da informação, ou seja, ter como objetivo central em todas as ações como colaborador da 4CO o respeito aos direitos humanos e liberdades fundamentais, respeitando ao máximo o indivíduo titular dos dados a serem tratados. Esses princípios devem ser espelhados na conduta e na tecnologia empregadas em todos os projetos.

- Ao trabalhar em um projeto, o colaborador deve sempre se pautar pelo princípio "coletar apenas o necessário". As pesquisas realizadas ou bancos de dados requeridos ao cliente têm de atender ao estritamente necessário exigido pelo projeto.

- Sempre que possível, evitar coletar e tratar dados sensíveis, como dados de saúde, etnia, religião etc. Se o projeto exige esse tipo de dado, ou se trata de temas sensíveis como sexualidade, racismo, assédio etc no ambiente de trabalho, os cuidados referentes a local de armazenamento e modo de envio desses dados precisam ser redobrados.

- O compartilhamento de dados pessoais tratados com colegas da equipe deve ocorrer apenas quando necessário e com quem possui autorização para tal. Em outras palavras, o compartilhamento de dados tratados deve ser restrito.

- Jamais o colaborador deve tratar dados pessoais a que tem acesso para finalidades diversas da sua atividade profissional. O uso de dados sem autorização significa inegável violação à privacidade e liberdade do titular de dados, com consequências jurídicas severas.

- Sempre que o colaborador receber uma base de dados de fonte diversa, recomenda-se entrar em contato com o líder do projeto

ou o Encarregado para validar a origem e o atendimento aos requisitos da LGPD.

- Do mesmo modo, quando possível, certificar que os dados analisados estão corretos e atualizados. Desconfiar de dados sem data de coleta, sem origem transparente e/ou incompletos.

- Toda vez que lidar com recebimento ou envio de dados pessoais a parceiros, fornecedores e clientes, o colaborador deve confirmar a existência de cláusulas contratuais a respeito de proteção de dados. Sugere-se, assim, que o líder do projeto comunique à equipe, desde o início, quais são os limites de armazenamento, compartilhamento e tratamento dos dados pessoais utilizados.

- No caso de qualquer dúvida a respeito do tratamento adequado de dados, da proteção contratual ou obediência à LGPD em dado projeto, entrar em contato com o Encarregado ou com a área jurídica, cujos contatos se encontram ao final deste Manual.

- Jamais utilizar dados pessoais tratados para fins discriminatórios, ilícitos ou abusivos.

- Sempre observar, em todas as atividades cotidianas, todos os princípios e obrigações descritos nesta Política de Privacidade e Tratamento de Dados.

Condutas técnicas

Além dos cuidados gerais acima descritos, os colaboradores devem buscar seguir as instruções técnicas listadas neste Manual de Boas Práticas. É possível evitar a maioria dos incidentes de segurança por meio de condutas adequadas, na maior parte de simples entendimento e aplicação:

- É dever de todo colaborador manter seguros os dados pelos quais é responsável. O primeiro passo para proteger dados é evitar usar senhas fáceis e sempre travar o computador ou smartphone quando não estiver utilizando. Trocar senhas periodicamente também é indicado.

- Ativar, sempre que possível, a autenticação em duas etapas em todas as plataformas que permitem essa função.

- Evitar, a todo custo, "espalhar" dados tratados em aplicativos e servidores distintos. Se é necessário enviar um conjunto de dados tratados a colegas, clientes ou parceiros, o compartilhamento deve ser realizado por apenas uma ferramenta.

- Priorizar armazenamento em "drives" seguros na nuvem. Evitar salvar arquivos em computadores, tablets e smartphones. De preferência, manipular dados em ambientes seguros e aprovados pelo líder do projeto ou Encarregado.

- Cuidado redobrado com o aplicativo WhatsApp: o app da Meta se tornou a ferramenta mais usada no Brasil para a vida pessoal e profissional. Sendo assim, é importante compreender os seguintes pontos:

    - ✔ O WhatsApp hoje é campeão em golpes no ambiente digital. Jamais escrever senhas ou enviar informações

sigilosas ou sensíveis no app, bem como enviar dados pessoais tratados.

- ✔ É comum a criação de grupos no WhatsApp ao se iniciar um projeto com a equipe. Isso é permitido, porém, o colaborador deve tratar o espaço do grupo no app tal qual uma extensão da área física da agência, sob as mesmas regras de conduta pessoal e desta Política de Privacidade.
- ✔ Ao término do projeto, jamais deixar “restos” de arquivos no app. Sempre apagar arquivos eventualmente armazenados em conversas ou grupos. Sempre apagar os grupos criados.

- <u>É absolutamente obrigatória a exclusão de dados não mais necessários de computadores, tablets ou smartphones</u> após atingir a finalidade da atividade de tratamento. Alguns exemplos de locais a serem excluídos:
  - ✔ Arquivos em servidores de e-mail, inclusive na “lixeira”.
  - ✔ Arquivos nas pastas “Downloads”, “Lixeira”, “Área de Trabalho”, “Temp” e em qualquer outra pasta criada em computadores.
  - ✔ Arquivos em aplicativos de mensagens.
  - ✔ Arquivos em “drives” na nuvem.

- O colaborador responsável pela contratação de sistemas ou serviços de tecnologia da informação que envolvam proteção de dados deve buscar <u>priorizar serviços ou sistemas que permitam a segmentação de acesso aos dados pessoais e que tenham boas garantias de proteção de dados</u>, tais quais uma Política de Privacidade clara e concisa, contrato com cláusulas de proteção, sistemas seguros e serviços de atendimento ao cliente para questões envolvendo proteção de dados. Ao trabalhar com parceiros de refino de dados, aplicar estas mesmas instruções.

- Eliminar papéis ou rascunhos desnecessários após o uso, idealmente picotados e rasgados. Jamais escrever dados pessoais em papéis.

- Se há dados pessoais armazenados de forma física, questionar a necessidade de mantê-los e se há segurança. Em caso negativo, eliminar todo material físico por incineração ou trituração segura.

- Tomar medidas de "higiene" digital: não abrir e-mails duvidosos ou clicar em links de origem suspeita; não fazer downloads de fontes não conhecidas; evitar o uso de pendrives ou outras mídias físicas quando lidar com dados tratados.

- Sempre tomar extremo cuidado com arquivos de áudio ou microfones, seja no envio de mensagens acerca de dados ou informações, seja na captação não intencional ou não autorizada de reuniões, ligações telefônicas etc.

- Quando houver a possibilidade, priorizar o uso de dados anonimizados, que impedem a identificação não autorizada de indivíduos.

- **NO CASO DE SUSPEITA DE INCIDENTE DE SEGURANÇA**: a conduta técnica a ser tomada na eventualidade de suspeita de incidente é i) parar o que está fazendo e priorizar o incidente; ii) imediatamente comunicar o Encarregado, por e-mail e telefone, da suspeita de incidente, com a maior riqueza de informações possível; iii) se certificar que o Encarregado recebeu a comunicação e está ciente do incidente.

Contatos p/ dúvidas ou comunicação de suspeita de incidente de segurança

Abaixo encontram-se os contatos do Encarregado e do representante da área jurídica para a solução de dúvidas a respeito da Política de Privacidade e Tratamento de Dados, bem como para comunicar suspeita de incidente de segurança e início do Plano de Resposta a Incidente (PRI):

Bruno Carramenha | encarregado e sócio-diretor
(11) 975-478-006 | bruno@4co.com.br

Fernando Melo Franco | área jurídica
(11) 971-492-217 | fernando@melofrancoadvogados.com.br

ANEXO 4 – MODELO DE CONSENTIMENTO PARA ENTREVISTAS E GRUPOS FOCAIS ONLINE

Introdução

Segundo a Lei Geral de Proteção de Dados, todo e qualquer tratamento de dados exige que o operador/controlador tenha obtido consentimento do titular para tratar dados de acordo com a finalidade do tratamento informada.

Em razão da necessidade de tratamento de dados durante entrevistas e grupos focais online para fins de pesquisa qualitativa, os participantes devem ser informados previamente da finalidade e do tratamento de dados. O texto abaixo deve ser utilizado como modelo para obtenção do consentimento.

Texto a ser inserido nos invites enviados

Prezado(a),

Em conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), informamos que sua participação nesta atividade requer o consentimento para coleta e tratamento de seus dados pessoais.

Ao confirmar sua presença nesta entrevista ou grupo focal online, você declara estar ciente e de acordo com os seguintes pontos:

As informações fornecidas durante a atividade serão utilizadas exclusivamente para fins de pesquisa, análise ou desenvolvimento de produtos/serviços, respeitando os princípios da boa-fé, necessidade e transparência.

Poderão ser coletadas informações como relatos pessoais, opiniões, sugestões e, eventualmente, dados pessoais fornecidos durante a conversa.

Os dados coletados durante a entrevista/grupo focal serão armazenados em ambiente seguro, com acesso restrito, pelo tempo necessário para as finalidades aqui descritas.

Informamos que os dados poderão ser compartilhados com parceiros envolvidos no projeto, desde que igualmente comprometidos com a confidencialidade e com a LGPD, e, em hipótese alguma, as informações coletadas serão compartilhadas com seus colegas de trabalho ou com seu empregador.

Você poderá solicitar, a qualquer momento, acesso, correção, anonimização ou eliminação dos seus dados pessoais, por meio dos nossos canais de contato.

Caso não concorde com os termos acima, solicitamos que não participe da atividade.

Sua participação é voluntária e muito importante para o desenvolvimento deste trabalho.

ANEXO 5 – MODELO DE TERMO DE CONSENTIMENTO PARA ENTREVISTAS QUALITATIVAS PRESENCIAIS

Orientações para apresentação do termo de consentimento:

Antes de iniciar a atividade de grupo ou entrevista, informe verbalmente que será necessário assinar um termo de consentimento, em conformidade com a LGPD. Explique, de maneira simples:

- Que nada será gravado;
- Que as informações servem apenas para fins de pesquisa;

- Que os dados não serão compartilhados fora da equipe do projeto;

- Que a pessoa pode se recusar a participar ou se retirar a qualquer momento;

- Que seus dados e relatos serão armazenados e tratados de forma segura.

Após esclarecer os pontos acima, entregue o termo impresso a seguir e ofereça tempo para leitura adequada.

Termo de consentimento para tratamento de dados pessoais – 4CO

A 4CO, em conformidade com a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD), solicita seu consentimento para a coleta e tratamento de dados pessoais durante sua participação nesta atividade presencial.

Finalidade do Tratamento:

As informações fornecidas serão utilizadas exclusivamente para fins de pesquisa, análise ou desenvolvimento de produtos, serviços ou melhorias organizacionais.

Informações importantes:

- A atividade não será gravada em áudio ou vídeo.

- Serão coletadas apenas informações verbais, registradas por meio de anotações.
- Os dados serão armazenados de forma segura e utilizados apenas pela equipe autorizada.
- Suas respostas serão tratadas de forma confidencial e, sempre que possível, de forma anonimizada.
- Você poderá solicitar acesso, correção ou exclusão dos dados a qualquer momento.

A participação é voluntária e você poderá desistir a qualquer momento, sem qualquer prejuízo.

Ao assinar este termo, você declara que:

- Foi devidamente informado(a) sobre o objetivo da atividade;
- Concorda com a coleta e uso das informações fornecidas;
- Autoriza o tratamento dos dados nos termos descritos.

Nome completo do participante:
_____
Documento (RG ou CPF):
_____
Assinatura: _____
Data: ____ / ____ / _____

ANEXO 6 – MODELO DE COMUNICAÇÃO DA EXCLUSÃO DO BANCO DE DADOS

Introdução

A Lei Geral de Proteção de Dados dispõe que ao término do tratamento de dados pessoais, todos os dados deverão ser eliminados. A principal hipótese de término de tratamento de dados ocorre quando a finalidade do tratamento

for atingida. Nesse caso, após a eliminação dos dados, o cliente deverá ser informado acerca da exclusão dos dados pessoais coletados durante a execução do contrato.

Texto a ser enviado para o cliente quando da exclusão dos dados pessoais

Prezado(a),

Gostaríamos de informar que, conforme previsto na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD), todos os dados pessoais e/ou sensíveis fornecidos pelo(a) [nome do cliente/empresa] ou por seus colaboradores no contexto da execução do nosso contrato [diagnóstico de cultura, implementação etc.], no qual foram realizadas(os) [pesquisas, entrevistas, grupos focais etc.], foram excluídos de nossos sistemas e registros diante do alcance da finalidade para a qual foram coletados.

Atenciosamente,

ANEXO 7 – MODELO DE TERMO DE CONSENTIMENTO PARA FORMAÇÃO DE BANCO DE DADOS DE LEADS

TERMO DE CONSENTIMENTO PARA TRATAMENTO DE DADOS PESSOAIS – 4CO

Ao preencher este formulário, você concorda com a coleta, o armazenamento e o uso dos seus dados pessoais pela 4CO, nos termos da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD).

Finalidade do Tratamento:

Seus dados (como nome, e-mail, telefone e empresa, entre outros) serão utilizados exclusivamente para fins de comunicação institucional e comercial, incluindo o envio de conteúdos, convites para eventos, newsletters e ofertas de produtos ou serviços da 4CO que possam ser do seu interesse.

Compartilhamento:

A 4CO se compromete a não compartilhar seus dados com terceiros sem seu consentimento prévio, salvo em casos de obrigação legal ou quando necessário para execução das finalidades acima, respeitando sempre a confidencialidade e a segurança das informações.

Segurança dos Dados:

A 4CO adota medidas técnicas e administrativas adequadas para proteger seus dados contra acessos não autorizados, vazamentos, alterações ou qualquer forma de tratamento inadequado.

Seus Direitos:

Você poderá, a qualquer momento, solicitar acesso, correção, exclusão ou portabilidade de seus dados, bem como retirar este consentimento, por meio do e-mail: **contato@4co.com.br**

Declaro que li e compreendi os termos acima e autorizo, de forma livre, informada e inequívoca, o tratamento dos meus dados pessoais pela 4CO, para os fins aqui descritos.

_____

[ ] Concordo e autorizo o uso dos meus dados pessoais pela 4CO, conforme descrito neste termo.

Nome completo: _____

E-mail: _____

Assinatura:_____

Data: ____ / ____ / _____