POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

CARLOS PINTO ADVOCACIA ESTRATÉGICA

Garantir sua privacidade é um compromisso da CARLOS PINTO ADVOCACIA.

A CARLOS PINTO ADVOCACIA ESTRATÉGICA está comprometido em assegurar a privacidade dos dados pessoais coletados para realização das suas atividades, bem como cumprir a Lei Geral de Proteção de Dados (Lei 13.709/18), com o Estatuto da Advocacia (Lei 8.906/94) e demais regulamentos aplicáveis sobre o tratamento de Dados Pessoais, incluindo Dados Pessoais Sensíveis. Por isso, esta política de privacidade foi elaborada para explicar de maneira detalhada como as suas informações serão protegidas e como você pode nos ajudar nessa tarefa.

A fim de definir processos, técnicas e medidas organizacionais adequadas ao tratamento de dados legalmente permitido, contra perda, dano e destruição acidental de Dados Pessoais, incluindo Dados Pessoais Sensíveis, e, por fim, garantir que estes sejam devidamente protegidos, Carlos Pinto Advocacia Estratégica decidiu adotar um amplo Programa de Privacidade de Dados Pessoais, que inclui a presente Política de Privacidade e Proteção de Dados Pessoais como o seu documento matriz.

Quaisquer dúvidas sobre a legislação aplicável e sobre processos que envolvam o tratamento de Dados Pessoais pela Carlos Pinto Advocacia Estratégica, incluindo Dados Pessoais Sensíveis, deverão ser direcionadas ao “Encarregado de Dados”, cuja função é a supervisão da Política de Proteção de Dados, juntamente com o comitê próprio formado pelos gestores da Carlos Pinto Advocacia Estratégica.

A qualquer momento e sempre visando ao aprimoramento dos serviços, a CARLOS PINTO poderá atualizar a Política de Privacidade, que poderá ser verificada sempre em nosso site.

Saiba que ao continuar utilizando os serviços, você aceita os termos e condições de uso do SITE e da SARA, bem como esta Política de Privacidade.

DEFINIÇÕES

Para os fins da presente Política de Privacidade e Proteção de dados (“Política”), os termos e expressões a seguir deverão ter os significados definidos abaixo:

“LGPD” significa Lei Geral de Proteção de Dados (Lei 13.709/18);

“Estatuto da Advocacia” significa a Lei que dispõe sobre o Estatuto da Advocacia e a Ordem dos Advogados do Brasil (Lei 8.906/94);

“Comitê de Privacidade e Proteção de Dados” significa o comitê formado por colaboradores da Carlos Pinto Advocacia Estratégica, cuja função é apoiar na tomada de decisões referentes ao Programa de Privacidade de Dados Pessoais;

“Colaboradores - todos os colaboradores, incluindo empregados, sócios, prestadores de serviços, advogados associados, estagiários, aprendizes e qualquer outra pessoa que possua vínculo direto com o escritório;

“Titular de Dados” significa a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

“Dado Pessoal” significa informação relacionada a pessoa natural que permita de qualquer forma a identificar;

“Dado Pessoal Sensível” significa dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, bem como outros dados específicos considerados sensíveis mediante as leis e regulamentos próprios;

“Dado Anonimizado” significa dado relativo a titular que não permita a sua identificação pela utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

“Controlador de Dados” significa a instituição a qual compete as decisões referentes ao tratamento de dados pessoais;

“Operador de Dados” significa pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais;

“Encarregado de Dados” ou “DPO” significa pessoa indicada e pelo Operador de Dados para atuar como canal de comunicação com os titulares dos dados e com a Autoridade Nacional de Proteção de Dados (ANPD);

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

“Consentimento” significa manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

“Relatório de Impacto à Proteção de Dados Pessoais” ou “RIPD” ou “DPIA” significa documentação que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

“Autoridade Nacional de Proteção de Dados” ou “ANPD” significa órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional; e,

“Políticas Setoriais de Privacidade e de Proteção de Dados” significa políticas de privacidade e proteção de dados pessoais, estruturadas a partir da presente Política de Privacidade e Proteção de Dados, que endereçarão as especificidades de cada uma das áreas responsável pelo Tratamento de Dados Pessoais.

OBJETIVO

O objetivo da Política de Privacidade e de Proteção de Dados Pessoais é definir as principais regras para o Tratamento de Dados aplicáveis à Carlos Pinto Advocacia Estratégica, a fim de garantir um nível adequado de proteção dos Dados Pessoais tratados, por meio de ações de proteção, em alinhamento com a LGPD, com o Estatuto da Advocacia e demais regulamentos que estabeleçam regras sobre o tema, executadas por suas áreas internas.

FORO

A presente Política aplica-se à coleta e Tratamento de Dados Pessoais ocorridos no Brasil. Dessa forma, esta Política será regida, interpretada e executada de acordo com as Leis da República Federativa do Brasil, especialmente a Lei nº 13.709/2018, independentemente das Leis de outros estados ou Países, sendo competente o foro de Recife/PE, para dirimir qualquer dúvida decorrente deste documento.

QUAIS DADOS COLETAMOS SOBRE VOCÊ?

Nosso **site** coletam e utilizam alguns dados pessoais seus, de forma a viabilizar a prestação de serviços e aprimorar a experiência do usuário. Dados pessoais fornecidos pelo titular:

- Nome
- Data de Nascimento
- E-mail
- CPF
- Endereço
- Telefone

Podemos coletar outros dados similares aos do site da CPADV, quando você utiliza serviços específicos, tal como em interação com a SARA (nosso BOT) ou alguma de nossas landing pages e formulários.

DADOS DE TERCEIRO

Alguns dos seus dados podem ser obtidos por nós através de fontes disponíveis ao público, prestadores de serviços e nossos parceiros. O tratamento desses dados estarão sempre de acordo com a legislação aplicável.

DADOS DE MENORES

Sabemos o quanto é importante a privacidade e proteção dos Dados de menores. Por isso, não será permitido que menores criem cadastro no nosso site, caso o façam os menores devem estar representados ou assistidos pelos responsáveis legais, na forma da lei.

Se, por um acaso, for necessária a coleta de dados de menores, esses serão tratados com o maior grau de segurança possível pela CPADV e deverá ter uma solicitação de autorização do responsável legal.

SEUS DADOS PODEM SER COMPARTILHADOS?

Seus dados poderão ser compartilhados com nossos parceiros comerciais.
AJUDA TRIBUTÁRIA – CNPJ -19.831.633/0001-70
EMPRESÔMETRO – CNPJ – 12.906.174/0001-05
CAPN – CNPJ – 13.295.961/0001-12
IBPTAX – 08.611.302/0001-08
IBPT Educação – CNPJ – 30.059.261/0001-48
E com nossa agência de marketing/comunicação.
Estes recebem seus dados apenas na medida do necessário para a prestação dos serviços contratados e nossos contratos são orientados pelas normas de proteção de dados do ordenamento jurídico brasileiro. Tendo em vista a preservação de sua privacidade, a CPADV não compartilhará seus dados pessoais com nenhum terceiro não autorizado.

APLICAÇÃO

A Política se aplica a todas as formas de Tratamento de Dados Pessoais na CPADV relacionadas às suas atividades, incluindo, mas não limitadas:

(i) à contratação de profissionais para compor o seu quadro de Colaboradores CPADV;

(ii) à contratação de fornecedores de serviços e de materiais;

(iii) à contratação de serviços jurídicos junto a clientes;

(iv) à manutenção das condições de segurança e de saúde necessárias ao exercício das suas atividades;

(v) ao desenvolvimento de novas linhas de atuação;

(vi) ao relacionamento com outros escritórios de advocacia, com a OAB e outras organizações;

(vii) ao relacionamento com todos os órgãos de governo, em todas as suas esferas, sendo da administração pública direta ou indireta, e;

(viii) ao seu relacionamento com a comunidade em que está inserida.

A presente Política engloba todos os tipos e as categorias de Dados Pessoais tratados pela CPADV, incluindo Dados Pessoais Sensíveis, coletados de Colaboradores CPADV; candidatos a vagas ofertadas pela CPADV; fornecedores; clientes; fornecedores e clientes em prospecção; parceiros comerciais; visitantes e quaisquer outras partes relacionadas

PRINCÍPIOS PARA O TRATAMENTO DOS DADOS

O Tratamento de Dados Pessoais sob responsabilidade da CPADV deverá ser realizado de acordo com as leis aplicáveis, bem como com a presente Política, observando os seguintes princípios:

(i) Os Dados Pessoais, incluindo os Dados Pessoais Sensíveis, devem ser obtidos de forma justa e legal. Sempre que necessário, o Consentimento expresso do Titular dos Dados deverá ser obtido de forma clara e inequívoca. O Titular dos Dados tem o direito à informação sobre os dados tratados, exceto se sua disponibilização for impossível ou exigir esforço desproporcional da CPADV;

(ii) A coleta de Dados Pessoais deve ser realizada apenas com finalidades específicas, explícitas e legítimas, sendo vedado o tratamento dos dados para outros fins. O compartilhamento dos dados com terceiros será para as finalidades previamente especificadas ou de outra forma permitida ou exigida pelas leis aplicáveis;

(iii) A CPADV implementará os controles e procedimentos técnicos e organizacionais apropriados para garantir a segurança dos Dados Pessoais, incluindo os Dados Pessoais Sensíveis, e evitar acesso ou divulgação não autorizados, que poderiam resultar em eventual alteração, destruição acidental ou ilegal, perdas dos dados e todas as demais formas ilegais de Tratamento de Dados. Considerando as obrigações legais e boas práticas, as medidas técnicas devem ser adotadas para garantir um nível de segurança apropriado aos riscos representados pelo Tratamento e natureza dos Dados Pessoais a serem protegidos;

(iv) A coleta dos Dados Pessoais, incluindo Dados Pessoais Sensíveis, deve ser adequada, relevante e limitada às finalidades e propósitos para os quais são coletados e/ou processados;

(v) A retenção dos Dados Pessoais, incluindo Dados Pessoais Sensíveis, deve ser por período não maior que o indispensável para as finalidades específicas para que foram obtidas, exceto quando exigido prazo diverso pela lei ou regulamento aplicável ou quando período diferente constar no Consentimento específico obtido;

(vi) Em sendo necessário o DPIA, este deverá ser elaborado incorporando os princípios do art. 6º. da LGPD, e (finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não-discriminação; responsabilização e prestação de contas);

(vii) Devem ser implementados procedimentos para garantir repostas imediatas às indagações dos Titulares dos Dados, assegurando o adequado exercício do direito de acesso, retificação e recusa ao Tratamento de Dados, exceto quando a LGPD de outra forma autorizar.

BASES LEGAIS

São bases legítimas para o Tratamento de Dados Pessoais pela CPADV:

(i) Consentimento inequívoco pelo Titular dos Dados;

(ii) Para o cumprimento de obrigação legal ou regulatória pela CPADV;

(iii) Quando solicitado e devidamente justificado pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas;

(iv) Execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o Titular dos Dados ou, a pedido do Titular dos Dados;

(v) Proteção da vida ou da incolumidade física do Titular dos Dados ou de terceiros;

(vi) Exercício regular de direitos da CPADV em processo judicial, administrativo ou arbitral;

(vii) Para a proteção do crédito, e;

(viii) Interesses legítimos da CPADV ou de terceiros (incluindo seus clientes), exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

São bases legítimas específicas para o Tratamento de Dados Pessoais Sensíveis pela CPADV:

(i) Consentimento específico, destacado e inequívoco pelo Titular dos Dados, ou de seu representante legal, quando aplicável, para as finalidades específicas;

(ii) Para o cumprimento de obrigação legal ou regulatória pela CPADV;

(iii) Quando solicitado e devidamente justificado pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas;

(iv) Exercício regular de direitos da CPADV e de seus clientes, inclusive em contrato e em processo judicial, administrativo e arbitral;

(vi) Proteção da vida ou da incolumidade física do Titular do Dado ou de terceiros;

(vii) Garantia da prevenção à fraude e à segurança do Titular dos Dados, em processos de identificação e autenticação de cadastro em sistemas eletrônicos, e;

(ix) Demais leis específicas aplicáveis ao Tratamento de Dados.

CONTRATADOS

Nos casos em que o Tratamento for realizado por um Operador de Dados em nome da CPADV, a CPADV escolherá um subcontratado que tenha condições técnicas de segurança e organizacionais suficientes para garantir que o Tratamento será executado de acordo com esta Política. A CPADV requererá a manifestação de concordância dos subcontratados em relação a presente Política de Privacidade e Proteção de Dados Pessoais.

TRANSFERÊNCIA DE DADOS INTERNACIONAIS

Na transferência de Dados Pessoais para fora do país a CPADV deverá observar, principalmente, mas não somente, as seguintes disposições:

(i) Os países ou instituições estrangeiras destinatários devem proporcionar grau de proteção aos Dados transferidos, conforme previsto na LGPD;

(ii) A CPADV deve garantir que o Operador de Dados estrangeiro apresente as condições para o cumprimento dos princípios e direitos dos Titulares dos Dados nos termos da LGPD e da presente Política de Privacidade de Dados, seja contratualmente ou pela apresentação de evidências documentais.

Você consente, dessa forma, que os seus Dados poderão ser transferidos, armazenados e tratados no Brasil ou em território estrangeiro pela CPADV ou por Parceiros, de acordo com essa Política. Onde quer que seus Dados sejam transferidos, armazenados ou tratados por nós ou por nossos Parceiros, saiba que tomaremos as medidas técnicas e organizacionais de segurança e confidencialidade e as proteções para garantir um nível adequado de proteção de Dados.

ARMAZENAMENTO DE DADOS

Os Dados Pessoais coletados e tratados poderão ser hospedados em servidores locais e/ou em servidores de terceiros e/ou em provedores de hospedagem na nuvem. A CPADV e qualquer terceiro que venha a estar envolvido neste processo implementam tecnologias e políticas de segurança para salvaguardar a privacidade de seus dados pessoais contra acesso não autorizado ou a utilização indevida.

DIREITOS DOS TITULARES DOS DADOS PESSOAIS

Em cumprimento à regulamentação aplicável, no que diz respeito ao tratamento de dados pessoais, em especial a Lei Geral de Proteção de Dados (Lei Federal nº 13.709/2018), a CPADV respeita e garante ao Usuário, a possibilidade de apresentação de solicitações baseadas nos seguintes direitos:

(i) A confirmação da existência de tratamento;
(ii) O acesso aos dados;
(iii) A correção do nome, CPF, idade, telefone e endereço quando incompletos, inexatos ou desatualizados;
(iv) A anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a Lei;
(v) A eliminação dos dados tratados com consentimento do Usuário, exceto nas hipóteses de guarda legal e outras dispostas em Lei;
(vi) A obtenção de informações sobre as entidades públicas ou privadas com as quais a CPADV compartilhou seus dados;
(vii) A informação sobre a possibilidade de não fornecer o seu consentimento, bem como de ser informado sobre as consequências, em caso de negativa;
(viii) A revogação do consentimento;
(ix) Oposição ao tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento e em desconformidade com a lei.

COMO VOCÊ PODE EXERCER SEUS DIREITOS DE TITULAR?

Parte destes direitos poderá ser exercida diretamente pelo Usuário, a partir da gestão de informações sobre sua conta, enquanto outros dependerão do envio de solicitação para posterior avaliação e adoção de demais providências pela CPADV.

Você deve entrar em contato com a *CPADV* através dos seguintes meios disponíveis:

E-mail:- cpadv.sac@gmail.com / lgpd@carlospintoadv.com / gilvan@carlospintoadv.com

Endereço: Empresarial Camilo Brito – R. Arnóbio Marquês, 253 – Sl 1803 – Santo Amaro, Recife – PE, 50100-130

De forma a garantir a sua correta identificação como titular dos dados pessoais objeto da solicitação, é possível que solicitemos documentos ou demais comprovações que possam comprovar sua identidade. Nessa hipótese, você será informado previamente.

AÇÕES PARA IMPLEMENTAÇÃO DA POLÍTICA

A CPADV realiza programa de treinamento para orientação de seus Colaboradores CPADV sobre a cautela e os processos necessários para o Tratamento dos Dados Pessoais, nos termos desta Política. A relevância da proteção de dados pessoais será, para além do programa de treinamento, reiterada no dia-a-dia da CPADV, principalmente compartilhando exemplos práticos através de sessões de conscientização.

Os treinamentos terão como base, no mínimo, a presente Política, o Estatuto da Advocacia e a LGPD.

A CPDAV possui Encarregados de Dados, Gilvan Soares e Francisco Castro, que poderão serem contatados pelos e-mails: lgpd@carlospintoadv.com e gilvan@carlospintoadv.com

São as atribuições e responsabilidades dos Encarregados, sempre atuando com independência, imparcialidade, decoro e boa-fé:

-Convocar e participar de reuniões do Comitê de Privacidade.

-Levar temas à discussão do Comitê de Privacidade, como necessidade de avaliação, implantação ou revisão de novas normas, processos e políticas.

-Levar conclusões, solicitações e resultados da atuação do Comitê de Privacidade às instâncias de decisão competentes do Escritório).

-Receber e dar encaminhamento interno a comunicações, requisições e intimações da ANPD – Autoridade Nacional de Proteção de Dados.

-Apresentar resposta do Escritório a comunicações, requisições e intimações da ANPD (após aprovação das instâncias de decisão competentes).

-Comunicar incidentes de segurança à ANPD em nome do Escritório (após aprovação das instâncias de decisão competentes).

-Atuar como canal de comunicação entre a ANPD e o Escritório em procedimentos administrativos.

-Receber e dar encaminhamento interno a solicitações e reclamações de titulares de dados pessoais. • Apresentar resposta do escritório a solicitações e reclamações de titulares de dados pessoais (após aprovação das instâncias de decisão competentes).

-Esclarecer dúvidas de titulares de dados pessoais quanto às práticas do Escritório com relação a seus dados pessoais.

-Comunicar incidentes de segurança aos titulares de dados pessoais em nome do Escritório (após aprovação das instâncias de decisão competentes).

-Orientar os colaboradores, contratados e terceirizados do Escritório com relação às políticas e práticas em vigor do Escritório relativas à privacidade e proteção de dados pessoais.

-Participar como consultor na revisão e no estabelecimento de processos do Escritório que possam trazer risco relevante à privacidade ou à proteção de dados pessoais de quaisquer pessoas (e.g. vazamentos, desvio de finalidade e tratamento ilícito de dados pessoais).

-Aconselhar as instâncias de decisão do Escritório com relação a comunicações, requisições e intimações da ANPD, solicitações e reclamações de titulares e incidentes de segurança, bem como em outras decisões que possam ter impacto à privacidade ou à proteção de dados pessoais de quaisquer pessoas.

-Controlar periodicidade e coordenar as revisões de registros de operação de tratamento.

-Controlar a periodicidade e coordenar as revisões de políticas e normas internas relativas à privacidade, proteção de dados pessoais e segurança de informação.

-Coordenar projetos de implantação de soluções para inadequações à legislação e regulamentos de proteção de dados pessoais.

-Acompanhar ou coordenar o acompanhamento da evolução das leis, regulamentos e boas práticas de privacidade, proteção de dados pessoais e segurança de informação.

-Participar na elaboração e revisão de cláusulas, minutas e documentos relacionados com o compartilhamento e transferência de dados pessoais.

-Participar na seleção ou elaboração de critérios de seleção de prestadores de serviços com potencial de risco relevante à privacidade e proteção de dados pessoais.

-Participar da elaboração e revisão de políticas e avisos de privacidade do Escritório para colaboradores, consumidores, usuários de sites etc.

-Auditar processos e práticas relativas à privacidade, proteção de dados pessoais e segurança de informação e levar suas conclusões às instâncias de decisão.

-Auditar prestadores de serviços com potencial de risco relevante à privacidade e proteção de dados pessoais.

-Realizar ou dirigir a realização de avaliações de interesse legítimo (“LIA”), avaliações de impacto à privacidade (“PIA”), e outras avaliações de riscos relacionados à proteção de dados pessoais, discutir seus resultados com os líderes dos projetos afetados e, se necessário, levar suas conclusões às instâncias de decisão.

-Realizar ou dirigir a realização de relatórios de impacto à proteção de dados pessoais (“RIPD” / “DPIA”) e obter aprovação das instâncias de decisão competentes para seu encaminhamento à ANPD.

-Ser informado de todas as novas atividades e processos do Escritório que tenham potencial de risco relevante à privacidade e proteção de dados pessoais.

-Recomendar a realização de LIAs, PIAs, RIPDs e outras avaliações de riscos à privacidade e proteção de dados pessoais para processos ou atividades do Escritório que, em sua percepção inicial, tenham possibilidade de resultar em danos.

-Constituir e participar em grupos de trabalho relacionados a melhorias na gestão de privacidade e mitigação de riscos à privacidade e proteção de dados pessoais.

-Solicitar e ter acesso a informações relevantes às suas atribuições, independentemente de sua classificação de confidencialidade.

-Participar do estabelecimento e revisão de processos e diretrizes de minimização de dados pessoais, eliminação de dados pessoais, “privacy by design” (i.e. garantir a proteção de dados pessoais desde a concepção de um projeto/atividade) e “privacy by default” (i.e. garantir o maior nível de privacidade possível quando houver alternativas ou escolhas).

Para apoiar os encarregados, a CPADV possui um Comitê de Privacidade e Proteção de Dados Pessoais, composto por 6 membros de áreas diferentes do escritório. O Comitê tem diversas responsabilidades, como:

- Acompanhar indicadores e planos de ação do Programa de Privacidade;

- Discutir e tomar decisões sobre novas atividades de tratamento de dados pessoais;

- Nivelar conhecimento sobre privacidade com todos os colaboradores;

- Assegurar o comprometimento dos colaboradores e parceiros institucionais com o Programa de Privacidade;

- Analisar as questões relativas à privacidade e proteção de dados trazidas pelo Encarregado ou por outras pessoas do Escritório,

-Discutir e participar da elaboração de normas, políticas, relatórios e documentos, entre outros assuntos correspondentes ao tema de privacidade e proteção de dados pessoais.

COMO PROTEGEMOS OS SEUS DADOS E RESPONSABILIDADE

A CPADV adota políticas e programas de conformidade, segurança e controle a fim de evitar violações à LGPD, prevenindo, detectando, monitorando e abordando violações em potencial, incluindo aqui as Políticas Setoriais de

Privacidade e Proteção de Dados Pessoais. Apesar disso, não é possível garantir a segurança de qualquer transmissão de dados pela internet.

Por esta razão, a CPADV não será responsável por quaisquer perdas de dados do USUÁRIO/CLIENTE, inclusive decorrentes de caso fortuito, força maior, ocorridas em virtude de invasões ao SITE/SARA e quebra de segurança por parte de terceiros não autorizados.

A CPADV empenhará seus melhores esforços para garantir que informações pessoais não sejam acessadas por terceiros de maneira indevida e estranha a esta Política de Privacidade.

REGISTRO DE RECLAMAÇÕES

A CPADV manterá um processo interno, centralizado no Encarregado, para recebimento de reclamações sobre o Tratamento de Dados Pessoais.

Os Titulares dos Dados, em caso de suposta ocorrência de Tratamento de seus Dados Pessoais de forma ilegal, inapropriada ou contrária à presente Política, deverão apresentar ao Encarregado a sua reclamação.

A CPADV manterá em seu site da internet pelo menos uma das ferramentas abaixo para que os Titulares de Dados possam registrar suas reclamações/solicitações direcionados ao Encarregado: (i) gilvan@carlospintoadv.com

As reclamações/solicitações serão avaliadas e respondidas nos prazos estabelecidos na LPGD que poderá ser entre 72 horas até 5 dias úteis.

ASSISTÊNCIA MÚTUA E COOPERAÇÃO COM A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

A CPADV cooperará com a ANPD em temas relacionados à privacidade de Dados Pessoais sob seu Tratamento, dentro dos limites da LGPD, mantendo seu direito ao contraditório. Nesse sentido adotará, dentre outras, as seguintes medidas:

(i) Informação dos dados de contato do DPO;

(ii) Disponibilização de Colaboradores CPADV para diálogo com a ANPD;

(iii) Revisitando de forma regular e efetiva o procedimento interno em atenção às diretrizes estabelecidas pela ANPD;

(iv) Respondendo às solicitações por informações ou reclamações; (v) Aplicando recomendações ou diretrizes estabelecidas.

A CPADV observará as decisões da ANPD, mas nunca renunciando ao seu direito ao contraditório.

Caso a ANPD solicite informações ou determine alguma ordem, qualquer colaborador que receba a informação/ordem deverá informar imediatamente ao Encarregado. O Encarregado deverá elaborar a resposta à Autoridade, contando com o suporte dos Colaboradores CPADV, Operadores de Dados, prestadores de serviços eventualmente envolvidos, administradores, responsáveis e/ou, se necessário, o Comitê de Privacidade e Proteção de Dados.

O Encarregado será o contato direto e primário entre a CPADV e a ANPD

CPADV COMO OPERADORA DE DADOS NO TRATAMENTO DE DADOS PESSOAIS

Na eventualidade da CPADV atuar como Operadora de Dados no Tratamento de Dados Pessoais, incluindo Dado Pessoal Sensível, serão observadas, sempre que aplicável, as regras estabelecidas pela presente Política, sem que isso implique que a CPADV assuma a condição de Controlador de Dados desses dados.

COMO ENTRAR EM CONTATO COM A AUTORIDADE APROPRIADA

Se você deseja relatar uma reclamação ou se achar que a CPADV não abordou sua preocupação de maneira satisfatória, entre em contato com a ANPD – Autoridade Nacional de Proteção de Dados Pessoais.

E-mail: anpd@anpd.gov.br
Endereço: Autoridade Nacional de Proteção de Dados
Esplanada dos Ministérios, Bloco C, 2º andar, CEP 70297-400 - Brasília – DF.

POLÍTICA DE SENHA E CONTROLES DE ACESSO

Interno

- CRM: Acesso através de senha criando pelo colaborador interno. Observar os critérios de boas práticas e sobre como formular senhas fortes e a importância de não compartilhamento delas.
-E-MAIL: Acesso através de senha com redefinições periódicas pelo responsável de T.I da empresa.
- DRIVE: Acesso através de link de permissão dado à determinado e-mail. A permissão pode ser dada à pasta ou ao documento. Deve ser realizado aconselhamento sobre a importância de não compartilhamento indevido do link.
- ASTREA: Acesso via senha criada pelo usuário. Observar os critérios de boas práticas e sobre como formular senhas fortes e a importância de não compartilhamento delas.

Externo

- CRM: Acesso através de senha criada pelo usuário, podendo haver consulta apenas na sua área, não sendo concedido acesso aos dados de outros clientes.

-DRIVE: Acesso através de link de permissão. A permissão deverá ser dada apenas ao documento ou pasta sendo controlado o acesso apenas como leitor.
-ASTREA: Acesso através de senha criada pelo usuário, podendo haver consulta apenas na sua área, não sendo concedido acesso aos dados de outros clientes.

Adendos:

a) Todas as autorizações de acesso devem ser controladas pelo T.I. que realizará o controle delas após a aprovação do HEAD responsável pelo usuário externo.
b) O HEAD deverá informar ao T.I. sobre o cadastramento ou descadastramento de acessos de usuários externos que estejam sob sua tutela.
c) Os sistemas, serviços e dispositivos do ambiente tecnológico da CPADV devem ser configurados para que os padrões de senha forte sejam exigidos na criação, conforme as recomendações abaixo:

I. Tenham no mínimo 6 (seis) caracteres;
II. Tenham caracteres numéricos e alfabéticos;
III. Não deve haver repetição de letras ou números na definição de senha, ou seja 3 (três) ou mais caracteres iguais sequenciados (ex: 111aaabbb);
IV. As digitações das senhas devem ser mascaradas na tela, armazenadas e trafegadas de forma criptografada, pelo sistema ou aplicação;

Boas práticas para criação de senhas

a) Evitar a utilização de:
   - Nomes, sobrenomes, nomes de contas de usuários de dados de membros da família;
   - Números de documentos ou de telefone
   - Placa de carros
   - Datas de aniversários, festivas, etc;
   - Sequência do teclado
b) Utilizar:
   - Números aleatórios;
   - Vários e diferentes tipos de caracteres;
   - Caracteres especiais;
   - Substituir uma letra por número com semelhança visual;
   - Frase longa com letras e números;
   - A primeira, segunda ou última letra de uma frase incluindo números

Adequação à política

Os novos projetos de desenvolvimento ou novas aquisições de sistemas devem seguir os padrões estabelecidos nesta política;

POLÍTICA DE CRIPTOGRAFIA

A política faz parte de um conjunto de documentos que compõem a Política de Segurança e Privacidade da Informação da CPADV. Os detalhes de determinados assuntos contidos nessa política estão regulados em outras práticas técnicas.

- Esta política deve ser lida por todos empregados e prestadores de serviços que atuem com as atividades descritas nela.
- Esta política institui regras sobre o uso efetivo e adequado de criptografia na proteção da informação.

Diretrizes gerias

a) Os controles criptográficos serão usados para assegurar, dentre outros:
    - A confidencialidade, a integridade e a autenticidade de informações sensíveis ou críticas que se encontrem armazenadas ou sob processo de transporte físico ou de transmissão eletrônica;
    - O não-repúdio: provara ocorrência de um evento ou ação alegados e suas entidade originárias, de forma a resolver disputadas sobre ocorrência ou não ocorrência do evento ou ação e do envolvimento das entidades no evento.
    - A autenticação: confirmar a identidade de usuários ou de sistemas automatizados.

b) A escolha dos tipos, da qualidade força de algoritmos, assim como a definição de que tipo de controle criptográfico é apropriado para cada propósito e processo de negócio, tomará como base, sempre que possível, o resultado do processo de gerenciamento de riscos de segurança da informação;

c) É proibida a implantação de controles criptográficos não homologados pelo setor de TI da EMAP ou utilizá-los de forma distinta aos procedimentos estabelecidos para tal finalidade;

d) O tráfego de login/senha de rede, durante a autenticação de usuários, e de informações classificadas como restritas entre as camadas envolvidas nos sistemas ou serviços disponibilizados pela EMAP deve ser protegido com o uso de mecanismos de criptografia como HTTPS, SSL, TLS e VPN.

e) Quando permitido por norma de tratamento da informação, documentos restritos que forem armazenados em dispositivos móveis (notebook, tablet, smartphone etc.) ou em mídias removíveis (cd, dvd, pen drive etc.) devem ser criptografados para evitar a sua divulgação indevida em caso de perda ou furto do equipamento ou da mídia.

Certificados digitais de uso interno

a) Além dos certificados digitais válidos na ICP-BRASIL, poderão ser utilizados outros certificados digitais. Respeitados os limites da lei, poderá ser aprovado o uso de certificados digitais em dispositivos de rede visando

interceptar com o objetivo de filtragem conteúdo previamente cifrado e que possa ser considerado inadequado, impróprio ou malicioso.

b) Os casos não previstos nesta política deverão ser encaminhadas para o setor de TI;
c) Os casos omissos serão resolvidos pelo setor de TI.

POLÍTICA DE COOKIES

Cookies são arquivos salvos em seu computador, tablet ou telefone quando você visita um site. Usa-se os cookies para fazer o site funcionar da melhor forma possível e sempre aprimorar os nossos serviços, permitindo uma boa execução das funcionalidades centrais, como segurança, gerenciamento de rede e acessibilidade.

Esses cookies podem ser coletados e armazenados assim que você inicia sua navegação ou quando usa algum recurso que os requer. Caso aceite os Cookies no seu navegador de internet, estará consentindo com o uso desses arquivos para que possamos agir de acordo com a nossa política de privacidade e cookies.

Caso não deseje que esses arquivos fiquem armazenados no seu computador, basta clicar no optout que aparece ao acessar o site ou você pode desabilitá-los alterando as configurações do seu navegador, mas saiba que isso pode afetar o funcionamento do site.

Prestadores de serviços de tecnologia poderão utilizar seus próprios cookies nos Serviços, com a nossa autorização, para prestação de serviços à CARLOS PINTO. Tais cookies coletam os seus dados nas nossas propriedades para as finalidades previstas nesta política.

POLÍTICA DE MESA LIMPA E TELA LIMPA

Para reduzir os riscos de acesso não autorizado, perda de informações ou danos às informações durante e fora do horário de expediente, a CPADV considera a adoção de uma política de “mesa limpa”, visando o resguardo de informações constante em documentos e/ou impressos durante a ausência do funcionário do seu local e/ou estação de trabalho.

A política deve considerar as classificações de segurança da informação, os riscos correspondentes e os aspectos culturais da organização. Informações deixadas sobre as mesas de trabalho são passíveis de serem danificadas ou destruídas de diversas formas.

O objetivo da política de “mesa limpa” é definir diretrizes que reduzam o risco de uma violação de segurança, fraudes e roubo de informações causadas por documentos que estão sendo deixados sozinhos nas instalações da empresa. Uma política de mesa limpa e tela limpa reduz o risco de acesso não autorizado, perda e dano da informação durante e fora do horário normal de trabalho.

O que Deve Ser Considerado?

- Os papéis (relatórios) devem ser armazenados em armários trancados e/ou em outras formas de mobiliário de segurança, quando não estiverem em uso, especialmente fora do horário do expediente;
- Computadores pessoais não devem ser deixados “logados” quando não houver usuário junto e devem estar protegidos por senhas e outros controles quando não estiverem sendo utilizados;
- Informações sensíveis ou confidenciais, quando impressas, devem ser retiradas imediatamente;
- Mantenha uma política de “mesa limpa” retirando papeis, anotações e lembretes da sua mesa de trabalho;
- Ao final do dia, ou no caso de ausência prolongada, limpar a mesa de trabalho;
- Não deixe papéis, livros ou qualquer informação na sua mesa quando não estiver no local;
- Armazene informações confidenciais em local apropriado (longe dos olhos de curiosos);
- Utilize um protetor de tela que solicite uma senha para acesso;
- As informações da sua organização são de sua responsabilidade! (Mesmo em sua casa!);
- Garanta que todos os documentos importantes, em caso de uma evacuação, estejam em local estrategicamente protegidos o que facilitará a recuperação;
- Deixe todos os documentos, no final do dia de trabalho, devidamente guardados/organizados;
- Documentos contendo informações de cliente devem estar trancados em gavetas ou armários;
- Descarte os itens referentes a informações dos clientes internos, externos, parte interessadas relevantes ou de propriedade da empresa em locais designados seguros;
- Sempre limpar sua área de trabalho antes de ir para casa, garantindo adequada organização dos itens/objetos manipulados ou relembrando/anotando para quem você repassou para arquivar/guardar;

POLÍTICA DE DISPOSITIVOS MÓVEIS

Você concorda em fazer sua parte para proteger a rede da empresa e os dados que estão armazenados ou acessados usando um dispositivo móvel. Como? Ao tomar medidas como estas:

- Fazer o melhor para proteger o dispositivo contra perda ou roubo.
- Informar imediatamente sobre um dispositivo perdido ou roubado.
- Mantendo o sistema operacional e os aplicativos atualizados e/ou verificando com a TI se você não tem certeza de como fazê-lo.
- Usando apenas aplicativos e ferramentas aprovados para acessar dados da empresa.

- Usando os programas e práticas de segurança fornecidos pela T.I. para evitar pirataria e/ou adulterações em software/configurações de segurança no dispositivo.
- Proteger o dispositivo com senhas ou outras formas que impeçam o acesso de terceiros não autorizados.
- Manter a área de trabalho virtual do dispositivo sem pastas que contenham nome ou informações referentes aos trabalhos desenvolvidos.
- Utilizar mecanismos de desligamento automático ou de “suspensão” das atividades em caso de afastamento do dispositivo ou inatividade por mais de 2 minutos, evitando assim que terceiros não autorizados possam ter acesso a quaisquer informações.
- Preste atenção para evitar malware e vírus, instalando apenas aplicativos e software confiáveis para garantir que dados confidenciais não sejam perdidos ou comprometidos.
- Deixe que os controles de segurança sejam implementados apenas pela T.I.
- Algumas senhas serão periodicamente alteradas pelo setor de T.I.
- Não use dispositivos moveis rooted ou jailbroken para acessar a rede corporativa. Estes são dispositivos que tiveram limitações e proteções removidas para que os usuários possam adicionar coisas como software não autorizado.
- Assegure, sempre que possível, que o dispositivo esteja configurado para manter separados os dados corporativos dos dados pessoais de forma segura.
- Em caso de viagens internacionais assegurar que está cumprindo todas as normas referentes à transferência de dados e tomando todas as precauções necessárias a conservação da incolumidade dos dispositivos.

Quem é elegível para acesso móvel?

Quem quer acesso móvel à rede da CPADV ou dados por dispositivo móvel deve solicitar aprovação de um colaborador, que entrará em contato com o setor de T.I., para realizar a autorização de acordo com o nível de classificação da pessoa que deseja utilizar a rede. Nem todos os usuários terão as mesmas permissões ou níveis de acesso. Você pode encontrar restrições com base no seu perfil, função ou departamento.

O que você pode e não pode fazer na rede corporativa?

- Você não deve usar o dispositivo para armazenar ou transmitir material ilícito ou informação pertencente a CPADV para outros fins que não sejam os do seu escopo de trabalho, ou para transferência à terceiros solicitados e autorizados.
- Não digitar mensagens (Whatsapp por exemplo) ou e-mail enquanto dirigir. É proibido pela empresa, independente de qualquer legislação local.
- Em dispositivos onde existe uma segregação clara e segura para dados e/ou aplicativos corporativos, as políticas da empresa serão aplicadas apenas aos

dados e aplicativos relacionados ao trabalho e a qualquer acesso corporativo à rede.
- Você poderá manter dados pessoais, tais como arquivos de texto ou fotos em seu dispositivo, lembrando sempre de segregar tais informações.

A CPADV poderá realizar uma limpeza remota se o dispositivo for perdido, roubado ou suspeito de estar comprometido. O dispositivo também pode ser apagado se não for compatível com as políticas da empresa, ou você não estiver mais vinculado à CPADV.
Onde os dados pessoais e corporativos e os aplicativos são mantidos separados, todas as tentativas serão feitas para limpar apenas os dados e aplicativos corporativos.

Penalidades

Qualquer usuário que tenha violado as políticas descritas neste documento pode estar sujeito a medidas disciplinares, tais como: ter negado o acesso às redes corporativas, aplicativos e dados, ter os dados removidos do dispositivo e o contrato de trabalho rescindido, além do cabimento de indenização compatível ao dano gerado e às sanções penais e cíveis cabíveis, além de denúncias as autoridades competentes, vide ANPD.

DATA E PRAZO DE VIGÊNCIA

A presente Política de Proteção de Dados entrará em vigor em outubro de 2021, por tempo indeterminado.

A presente Política poderá ser atualizada e alterada a qualquer tempo, sem aviso prévio.

DISPOSIÇÕES GERAIS

A implementação da presente Política de Privacidade de Dados e das ações dela decorrentes será objeto de auditorias internas periódicas.

Em caso de comprometimento dos Dados Pessoais tratados pela CPADV, todo e qualquer colaborador ou terceiro que tiver conhecimento deverá notificar imediatamente o Encarregado. Avaliados os riscos, caberá ao DPO, se aplicável, a comunicação à ANPD e aos Titulares dos Dados. Em havendo necessidade de notificação à ANPD, nesta deverão constar:

(i) a descrição do tipo e categoria dos Dados Pessoais afetados;

(ii) quais foram os Titulares de Dados envolvidos;

(iii) as medidas utilizadas para proteção dos dados, respeitados os limites dos segredos comerciais e industriais; bem como,

(iv) no caso de demora na resposta ao incidente, o motivo.

O Encarregado deve assegurar revisões e atualizações regulares da Política de Privacidade de Dados, por exemplo, como consequência de alterações na estrutura corporativa e no ambiente regulatório. Assim, a definição e atualização das medidas técnicas e organizacionais a serem implementadas no Tratamento dos Dados Pessoais, de acordo com as disposições legais, devem ser editadas com auxílio do encarregado e entrarão em vigor, apenas e tão somente com a sua revisão e aprovação.