FUTURE CARBON GROUP

Política de Privacidade e Proteção de Dados Pessoais

2022

Versão	01

Em suas operações diárias, o Grupo Future Carbon realiza uma variedade de atividades de tratamento de dados pessoais de seus Colaboradores, Administradores, Clientes, Fornecedores, parceiros de negócios, usuários de seu site na internet, e de outras partes interessadas.

Por estar absolutamente comprometido com os valores e princípios da liberdade, privacidade, intimidade, livre desenvolvimento da pessoa humana e titularidade dos dados pessoais, o Grupo Future Carbon estabelece a presente Política visando estar em plena conformidade com a Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) e, quando aplicável, à Regulação Geral de Proteção de Dados da União Europeia (*EU General Data Protection Regulation - GDPR*).

Neste documento, nós esclarecemos sobre as regras legais relevantes para nossas operações e descrevemos os princípios, diretrizes e medidas que adotamos na Companhia para garantir a conformidade com a lei.

Sumário

1. Objetivo

Esta política estabelece princípios e diretrizes que visam orientar os Administradores e Colaboradores do Grupo Future Carbon sobre como proceder na realização de operações de tratamento de dados pessoais, o respeito ao direito dos titulares, medidas de segurança da informação e boas práticas e sobre o relacionamento da Companhia com titulares, controladores, operadores e a Autoridade Nacional de Proteção de Dados.

2. Abrangência

Esta Política se aplica a todos os Profissionais e empresas integrantes do Grupo Future Carbon, independentemente de seu nível hierárquico e funcional ou local de atuação. Inclui, portanto, administradores (conselheiros e diretores), membros de comitês auxiliares, membros do conselho fiscal, executivos e colaboradores, estagiários, fornecedores, prestadores de serviços e demais terceiros que com ele se relacionam.

Da mesma maneira, esta Política também se aplica às *joint ventures*, acordos temporários e outras situações equivalentes nas quais a Companhia exerça influência na gestão.

3. Definições

Esta política observa as mesmas definições conceituais estabelecidas na LGPD, com destaque para:

i. Dado pessoal

Informação relacionada a pessoa natural identificada ou identificável;

ii. Dado pessoal sensível

Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

iii. Titular

Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

iv. Controlador

Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

v. Operador

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

vi. Encarregado de proteção de dados

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

vii. Tratamento de dado pessoal

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;

viii. Consentimento do titular

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

4. Princípios e diretrizes sobre tratamentos de dados pessoais

4.1. Colaboradores e Administradores do Grupo Future Carbon apenas estão autorizados a realizar tratamento de dados pessoais quando configurada uma ou mais das seguintes hipóteses:

i. mediante o fornecimento de consentimento pelo titular;
ii. para cumprir obrigação legal ou regulatória;
iii. quando necessário para a execução de contratos ou de procedimentos preliminares relacionados a contratos do qual seja parte o titular dos dados e a seu pedido;
iv. para o exercício regular de direitos em processo judicial, administrativo ou arbitral;
v. para a proteção da vida ou da incolumidade física do titular ou de terceiros;
vi. quando for necessário atender os interesses legítimos da Companhia em sua condição de controlador, nos casos autorizados na LGPD.
vii. Se envolver dados pessoais de crianças, através do consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

4.2. Colaboradores e Administradores do Grupo Future Carbon apenas estão autorizados a realizar tratamento de dados pessoais sensíveis quando configurada uma ou mais das seguintes hipóteses:

i. quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
ii. para cumprimento de obrigação legal ou regulatória pelo controlador;
iii. para o tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
iv. para fins de exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
v. proteção da vida ou da incolumidade física do titular ou de terceiros;
vi. para garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, exceto nos casos em que prevalecerem direitos e

liberdades fundamentais do titular que exijam a proteção dos seus dados pessoais.

4.3. O Grupo Future Carbon realiza suas operações de tratamento de dados pessoais de seus Colaboradores, Administradores, Clientes e outros interessados observando os seguintes fundamentos:

i. o respeito à privacidade;
ii. a autodeterminação informativa;
iii. a liberdade de expressão, de informação, de comunicação e de opinião;
iv. a inviolabilidade da intimidade, da honra e da imagem;
v. desenvolvimento econômico e tecnológico e a inovação;
vi. a livre iniciativa, a livre concorrência e a defesa do consumidor; e
vii. os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

4.4. Além disso, na condução das operações de tratamento de dados pessoais, o Grupo Future Carbon irá se pautar pelos seguintes princípios e diretrizes:

i. A Companhia apenas realizará tratamento de dados pessoais para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
ii. A Companhia garantirá a adequação e a compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
iii. As operações de tratamento serão limitadas ao mínimo necessário para a realização de suas finalidades;
iv. Será garantido aos titulares a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
v. Será respeitada a qualidade dos dados, entendida como a garantia aos titulares de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
vi. A Companhia também garantirá a transparência do tratamento, entendida como a garantia aos titulares de informações claras,

precisas e facilmente acessíveis sobre a realização do tratamento, ressalvando eventuais segredos comerciais e industriais;

vii. A Companhia irá adotar medidas de segurança técnicas e administrativas que sejam aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

viii. A Companhia se pauta pela prevenção, adotando medidas para evitar a ocorrência de danos decorrentes do tratamento de dados pessoais;

ix. A Companhia não realizará tratamentos de dados para fins discriminatórios ilícitos ou abusivos;

x. A Companhia, irá demonstrar, na condição de controlador, a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

5. Regras para obtenção e revogação do Consentimento do Titular para Tratamento de Dados Pessoais

5.1. Nas hipóteses em que a LGPD exige a obtenção do consentimento do titular para o tratamento de seus dados pessoais, este será obtido por escrito ou por outro meio que demonstre a manifestação de vontade concordante do titular.

5.2. O consentimento deverá ser manifestado de forma específica e destacada e referir-se claramente às finalidades determinadas do tratamento de dados, sendo vedada a obtenção de autorizações genéricas junto ao titular.

5.3. Caso for feita por escrito, a obtenção do consentimento do titular dos dados deverá observar o modelo de documento presente no Anexo I a esta Política.

5.4. Se o tratamento envolver dados pessoais de crianças, deverá ser antecedido de consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

5.5. Eventual pedido de revogação do consentimento apresentado por titular à Companhia deverá ser encaminhado ao Encarregado pelo

Tratamento de Dados Pessoais do Grupo Future Carbon, que avaliará sua adequação às hipóteses legais e decidirá se o atenderá, formalizando a decisão e comunicando o titular em qualquer caso.

6. Procedimento para atendimentos e pedidos de acesso dos titulares aos dados pessoais

6.1. O Grupo Future Carbon recebe, através de canal em seu site na internet, pedidos apresentados por titulares, sobre:

i. confirmação da existência de tratamento que utilize seus dados pessoais;
ii. acesso aos dados de sua titularidade;
iii. correção de dados incompletos, inexatos ou desatualizados;
iv. anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
v. portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
vi. eliminação dos dados pessoais tratados com seu consentimento, exceto nas hipóteses em que a LGPD autoriza sua conservação;
vii. identificação das entidades públicas e privadas com as quais a Companhia compartilhou seus dados;
viii. informação sobre a possibilidade de não fornecer consentimento para o tratamento de seus dados e sobre as consequências da negativa.

6.2. O pedido apresentado por um titular será encaminhado ao Encarregado pelo Tratamento de Dados Pessoais, que avaliará sua adequação às hipóteses legais e decidirá se o atenderá, formalizando a decisão e comunicando o titular em qualquer caso.

7. Transferência Internacional de Dados Pessoais

O Grupo Future Carbon apenas irá transferir dados pessoais por ela tratados para países ou organismos internacionais que proporcionem grau de

proteção adequado ao previsto na legislação brasileira e mediante garantias contratuais oferecidas e comprovadas pelo controlador de respeito aos princípios, direitos do titular e regime de proteção de dados previstos na LGPD.

8. Medidas de Segurança e Boas Práticas

8.1 O Grupo Future Carbon adota medidas de segurança técnicas e administrativas para evitar e coibir acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito dos dados pessoais que trata. Estas medidas são adotadas e incorporadas em nossos serviços desde a sua concepção (*privacy by design*).

8.2 Além disso, nas atividades de compartilhamento de dados que mantém com parceiros de negócios, como provedores de internet, de serviços de e-mail, de armazenamento em nuvem, entre outros, a Companhia busca selecionar aqueles que adotam rígidas medidas de segurança e boas práticas de proteção de dados e respeitam os princípios e regras previstos na LGPD.

8.3 Todos os dados que tratamos, estejam armazenados em nossos sistemas de Tecnologia da Informação (TI) ou em registros físicos, estão disponíveis apenas para membros da equipe com autorização legítima de acesso e estão protegidos contra acesso e processamento não autorizado e contra perda e corrupção.

8.4 A responsabilidade pela segurança e integridade de todos os Sistemas de TI e dos dados armazenados neles (incluindo, mas não se limitando à segurança, integridade e confidencialidade desses dados) é do Diretor de TI, salvo indicação expressa em contrário.

8.5 Todos os funcionários têm a obrigação de relatar falhas de conformidade de proteção de dados reais e potenciais ao Diretor de TI, que deve investigar a violação. Qualquer violação conhecida ou suspeita de envolver dados pessoais deve ser relatada ao Encarregado pelo Tratamento de Dados.

i. Diretrizes de segurança física e procedimentos

a. Registros em papel e documentos que contenham dados pessoais e informações confidenciais devem ser posicionados de forma a evitar ao máximo a visualização por parte de outras pessoas, por exemplo, através de janelas. Ao final do dia de trabalho, ou ao deixar sua mesa desocupada, os Colaboradores devem recolher todos os documentos em papel e guardá-los em segurança para evitar acesso não autorizado.
b. Salas de armazenamento, armários trancados e outros sistemas de armazenamento com travas devem ser usados para guardar registros em papel quando não estiverem em uso.
c. Documentos em papel contendo dados pessoais não devem ser deixados em mesas de escritório e salas de reunião, fora do período de trabalho ou da realização das reuniões.
d. Documentos em papel contendo dados pessoais não devem ser retirados das dependências da Companhia, exceto se isso for necessário para a realização de alguma atividade em que a apresentação física dos dados seja imprescindível (exemplo: cartórios).
e. A segurança física das dependências e dos sistemas de armazenamento deve ser monitorada e revista regularmente. Se algum Colaborador do Grupo Future Carbon entender que a segurança atual é insuficiente, ele deve informar o Encarregado pelo Tratamento de Dados o mais rápido possível.
f. As instalações do Grupo Future Carbon possuem controles de acesso supervisionado por porteiros, circuito interno de TV, crachás, uniformes, cartões de acesso, alarmes, entre outras barreiras físicas que visam dificultar acessos não autorizados.
g. Eventuais visitas às dependências do Grupo devem ser acompanhadas por um Colaborador e os visitantes nunca devem ser deixados sozinhos em áreas onde possam ter acesso a dados pessoais ou outras informações confidenciais.

ii. Sistemas de Tecnologia da Informação e Responsabilidades do Diretor de TI

São responsabilidades do Diretor de Tecnologia da Informação do Grupo:

a. garantir que todos os Sistemas de TI sejam avaliados e considerados adequados para o cumprimento dos requisitos de segurança da Companhia;
b. garantir que os padrões de segurança de TI dentro da Companhia sejam efetivamente implementados e revisados regularmente;
c. fornecer a todos os membros da equipe suporte e treinamento adequados em questões de segurança de TI e uso de sistemas de TI;
d. garantir que todos os membros da equipe tenham níveis de acesso aos sistemas de TI apropriados para cada membro, levando em consideração sua função, responsabilidades e quaisquer requisitos especiais de segurança;
e. receber reclamações relacionadas a questões de segurança de TI e tomar as medidas apropriadas em resposta, inclusive, no caso de quaisquer reclamações relacionadas a dados pessoais, informar o Encarregado de pelo Tratamento de Dados Pessoais;
f. tomar medidas proativas, sempre que possível, para estabelecer e implementar procedimentos de segurança de TI e conscientizar os membros da equipe;
g. monitorar toda a segurança de TI dentro da Companhia e garantir que sejam feitos backups regulares de todos os dados armazenados nos Sistemas de TI em intervalos regulares e que esses backups sejam armazenados em um local adequado fora das instalações da Companhia.

iii. Responsabilidades dos Colaboradores

a. Todos os membros da equipe devem cumprir os termos desta Política em todos os momentos ao usar os Sistemas de TI.

b. Computadores e outros dispositivos eletrônicos devem ser bloqueados quando não estiverem em uso para minimizar a perda ou divulgação acidental de dados.
c. Colaboradores devem informar imediatamente o Diretor de TI ou o Encarregado pelo Tratamento de Dados, sobre todas e quaisquer preocupações de segurança relacionadas aos Sistemas de TI que possam ou tenham levado a uma violação de dados.
d. Problemas técnicos (incluindo, mas não limitado a, falhas de hardware e erros de software) que possam ocorrer nos Sistemas de TI devem ser relatados imediatamente ao Consultor de TI.
e. Colaboradores não devem instalar nenhum software próprio sem a aprovação do Diretor de TI. Um software só poderá ser instalado quando essa instalação não representar risco de segurança para os Sistemas de TI e onde a instalação não violar quaisquer contratos de licença aos quais esse software possa estar sujeito.
f. Antes de qualquer uso de mídia física (por exemplo, cartões de memória USB ou discos de qualquer tipo) para transferir arquivos, o Colaborador deve certificar-se de que a mídia física foi verificada contra vírus.
g. Caso um vírus seja detectado, isso deve ser relatado imediatamente ao Diretor de TI (esta regra deve ser aplicada mesmo quando o software antivírus corrige automaticamente o problema).

iv. Segurança de Acesso

a. Todos os Colaboradores são responsáveis pela segurança dos equipamentos eletrônicos colocados pela Companhia à sua disposição e não devem permitir que seja usado por qualquer pessoa que não esteja sujeita a esta política.
b. Os dados pessoais do Grupo Future Carbon são protegidos por senhas, criptografia, firewall seguro e software antivírus, que visam proteger os sistemas de TI de invasões e outras formas de acessos não autorizados.
c. Todos os sistemas de TI (em particular dispositivos móveis) devem ser protegidos com uma senha ou código de acesso seguro, ou

outra forma de sistema de login seguro aprovado pelo Departamento de TI. Os métodos de login biométrico só podem ser usados se aprovados pelo Departamento de TI.

d. As senhas e informações de login são pessoais e somente podem ser utilizadas pelo respectivo Colaborador. Os Colaboradores não devem informar sua senha e informação de login, ou mesmo autorizar o uso de seus dispositivos, para outro colaborador ou terceiro.
e. Se você esquecer sua senha, deverá notificar o Diretor de TI para que seu acesso aos Sistemas de TI seja restaurado. Você deve configurar uma nova senha imediatamente após a restauração do acesso aos Sistemas de TI.
f. Você não deve anotar senhas se for possível lembrá-las. Se necessário, você pode anotar as senhas, desde que as armazene com segurança (por exemplo, em uma gaveta trancada ou em um banco de dados de senhas seguro). As senhas nunca devem ser deixadas em exibição para outras pessoas verem.
g. Computadores e outros dispositivos eletrônicos com telas e dispositivos de entrada do usuário (por exemplo, mouse, teclado, tela sensível ao toque etc.) devem ser protegidos com um bloqueio de tela que será ativado após um período de inatividade.
h. Todos os dispositivos móveis fornecidos pela Companhia devem ser configurados para travar, “dormir” ou providência similar, após um período de inatividade, exigindo senha, ou outra forma de login para desbloqueio.
i. Os Colaboradores devem estar cientes de que, se não realizarem o encerramento da sessão (“logoff”) e deixarem seus terminais sem vigilância, poderão ser responsabilizados pelas atividades de outro usuário em seu terminal em violação desta Política.

v. Segurança de Dados

a. Os dados pessoais tratados pelo Grupo Future Carbon serão criptografados ou protegidos de outra forma.

b. Todos os membros da equipe estão proibidos de baixar, instalar ou executar software de fontes externas sem obter autorização prévia do Diretor de TI que considerará solicitações de boa-fé para fins de trabalho. Isso inclui programas de mensagens instantâneas, protetores de tela, fotos, videoclipes, jogos, arquivos de música e abertura de documentos ou comunicações de origens desconhecidas.
c. Colaboradores podem conectar seus próprios dispositivos (incluindo, mas não limitado a, laptops, tablets e smartphones) à rede Wi-Fi do Grupo Future Carbon, desde que sigam os requisitos e instruções dos Técnicos de TI da Companhia. Todo o uso de dispositivos enquanto conectados à rede da Companhia ou qualquer outra parte dos Sistemas de TI está sujeito a todas as Políticas relevantes (incluindo, mas não se limitando a esta política). Qualquer técnico de TI pode, a qualquer momento, solicitar a desconexão imediata de quaisquer desses dispositivos sem aviso prévio.

vi. Armazenamento eletrônico de dados

a. Todos os dados portáteis, e em particular os dados pessoais, devem ser armazenados em unidades criptografadas usando métodos recomendados pelos técnicos de TI da Companhia.
b. Todos os dados armazenados eletronicamente em mídia física e, em particular, dados pessoais, devem ser armazenados de forma segura em uma gaveta trancada, armário ou similar.
c. Colaboradores não devem armazenar quaisquer dados pessoais tratado pela Companhia em qualquer dispositivo móvel, seja tal dispositivo pertencente ou não ao Grupo Future Carbon, sem a aprovação prévia por escrito do Diretor de TI. Você deve excluir os dados copiados em qualquer um desses dispositivos o mais rápido possível e certificar-se de que estejam armazenados nos Sistemas de TI da Companhia para que seja feito o backup.
d. Todos os dados eletrônicos devem ter um backup seguro feito até o final de cada dia de trabalho.

vii. Teletrabalho (*Homeworking*)

a. Colaboradores não devem levar dados pessoais e outras informações confidenciais para casa sem a permissão prévia do Encarregado pelo Tratamento de Dados, e só o fará quando houver medidas técnicas e práticas adequadas em sua casa para manter a segurança e a confidencialidade contínuas dessas informações.
b. Quando você tiver permissão para levar para casa dados pessoais ou outras informações confidenciais, você deve garantir que as informações são mantidas em ambiente seguro e trancado, onde não podem ser acessadas por familiares ou visitantes; e que todo o material confidencial que necessite de descarte seja triturado ou, no caso de material eletrônico, destruído de forma segura, tão logo passe qualquer necessidade de sua retenção.

viii. Uso de e-mails e aplicativos de mensagens

a. Dados pessoais tratados pela Companhia somente podem ser enviados por Colaboradores através de contas corporativas e de sistemas e/ou aplicativos baseados em criptografia.
b. Colaboradores devem ter cuidado adicional ao inserir endereços de e-mail onde os recursos de preenchimento automático podem sugerir endereços incorretos.

ix. Violações de segurança

a. Todas as preocupações, dúvidas, violações suspeitas ou violações conhecidas devem ser encaminhadas imediatamente ao Diretor de TI e ao Encarregado pelo Tratamento de Dados Pessoais. Todos os membros da equipe têm a obrigação de relatar falhas de conformidade de proteção de dados reais ou potenciais.
b. Ao receber uma comunicação ou notificação de uma violação, o Diretor de TI deve avaliar imediatamente o problema e deve tomar todas as medidas necessárias para responder ao evento. Em

seguida, o Diretor de TI deve comunicar detalhadamente o problema ao Encarregado pelo Tratamento de Dados Pessoais.

c. Os Colaboradores não devem, sob nenhuma circunstância, tentar resolver uma violação de segurança de TI por conta própria sem antes consultar o Diretor de TI.
d. Registros em papel perdidos ou roubados ou dispositivos móveis, computadores ou mídia física contendo informações pessoais ou confidenciais devem ser relatados imediatamente ao Diretor de TI.
e. Todas as violações de segurança de TI devem ser totalmente documentadas.

9. Encarregado pelo Tratamento de Dados Pessoais

As atividades e responsabilidades do Encarregado pelo Tratamento de Dados Pessoais consistem em:

i. receber reclamações e comunicações dos titulares dos dados, prestar esclarecimentos e adotar providências;
ii. receber reclamações e comunicações de outros Colaboradores e Administradores da Companhia, prestar esclarecimentos e adotar providências;
iii. receber comunicações da autoridade nacional de proteção de dados e adotar providências;
iv. orientar os funcionários e os contratados da Companhia a respeito desta Política e das práticas a serem adotadas em relação à proteção de dados pessoais.

Nome do Encarregado: Humberto Lima
E-mail: privacidade@futurecarbon.com.br

10. Infrações internais à Política

Em caso de indícios de violação às regras desta Política, será realizada a devida investigação pelo Departamento de Integridade em conjunto com o Encarregado pelo Tratamento de Dados Pessoais e, se comprovada a infração, serão aplicadas as medidas disciplinares cabíveis aos envolvidos, de acordo com

a legislação trabalhista, sem prejuízo de comunicação às autoridades competentes, quando aplicável.

11. Disposições gerais

É de competência do Conselho de Administração da Companhia alterar esta Política sempre que se fizer necessário.

Esta Política entra em vigor na data de sua aprovação pelo Conselho de Administração e revoga quaisquer documentos em contrário.

2022

Future Carbon Holding S.A