

## Procedimentos da LGPD

### 1 – Identificação

A **Carmo Artigos Esportivos Ltda – ME – CS Academia** é uma empresa que atua na área de Saúde, Disposição e Bem-estar fundada em 1993, e que se encontra atualmente sediada na cidade de Ribeirão Preto/SP, na Rua Pinheiro Machado, 1006 – Bairro Campos Elíseos.

CNPJ sob nº 72.810.989/0001-00.

Fone: (16) 99104-4966.

A **Carmo Artigos Esportivos Ltda – ME – CS Academia** utilizará neste procedimento o nome **C.A.E.L-ME** em todos os momentos necessários.

Em atendimento a Lei 13709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), estará neste documento, registrando todas as atividades e procedimentos elaborados.

### 2 – Forma de Atuação

Para atender a todas as exigências e necessidade de implementação solicitada pela LGPD, a **C.A.E.L-ME** desenvolveu diversas atividades e procedimentos que detalharemos a seguir.

Estas atividades e estes procedimentos, poderão ser renovados a qualquer momento, para podermos manter nosso sistema de proteção de dados pessoais atualizados.

#### 2.1 – Contratação de Consultoria

Devido à complexidade e necessidades para podermos atender a LGPD, a alta direção da **C.A.E.L-ME**, resolveu realizar a contratação de um consultor externo para auxiliar nas implementações necessárias.

#### 2.2 – Treinamento Inicial

Foi realizado como primeira atividade um treinamento com base na Lei 13709/2018 para a Gerente, conforme comprovante de treinamento disponibilizado pelo consultor contratado.

***Nota 1:** A partir deste momento, a Gerente, poderá realizar o treinamento dos outros colaboradores da organização.*

#### 2.3 – Data Mapping

A Gerente da **C.A.E.L-ME**, ficou responsável por preencher o formulário Data Mapping juntamente com o consultor externo.

Neste formulário, conseguimos definir as seguintes informações:

- **Qual setor ou departamento estamos analisando?** - Neste campo, foi informado o setor/departamento que está sendo analisado criticamente;
- **Tipo do dado pessoal coletado/tratado (CPF, identidade, endereço, dados de terceiros etc.)** - Ao analisar o setor/departamento, informamos todos os dados pessoais que ele tem acesso. Para isto, analisamos cada atividade desenvolvida, trazendo para o formulário uma informação detalhada de todas as informações pessoais que cada atividade o setor/departamento tem acesso;
- **Como agente de tratamento a organização será operador ou controlador?** – Neste campo, informamos em cada atividade desenvolvida, se é como operador ou controlador da informação;
- **Origem do dado (site, contrato etc.)** – Informamos, em cada situação encontrada, como o setor coleta as informações pessoais;

- **Qual a sua finalidade?** – Para qual motivo o setor/departamento coleta os dados pessoais identificados;
- **Armazenamento (como e onde é armazenado?)** – Informamos todas as formas de armazenamento dos dados pessoais identificados. Por exemplo: Se são digitais ou físicos, locais onde ficam armazenadas estas informações etc.;
- **O dado é classificado como sensível? Art. 5º, inciso II** – Quando há algum dado sensível, conforme o artigo 5º, inciso II do LGPD, deve deixar informado neste campo;
- **Base legal para o tratamento Art. 7º** - Ao identificarmos dados pessoais e analisarmos a informação encontrada, informamos neste campo, qual a base legal que utilizamos para este tratamento, conforme o artigo 7º da Lei 13709/2018. Importante: No campo disponibilizado no formulário, há a relação de todas as bases legais informadas na Lei;
- **Período de retenção dos dados** – Neste campo, identificamos qual o período pré-determinado para a retenção dos dados encontrados. Caso não exista, informamos como “Indeterminado”;
- **Outro colaborador ou outro setor da organização, tem acesso a estes dados?** – Caso, outros colaboradores ou outros setores da organização, tenham acesso aos dados coletados em um setor/departamento, informamos “Sim”. Caso, nenhum outro colaborador ou setor/departamento da organização, tenha acesso aos dados coletados, informar “Não”;
- **Se na pergunta anterior, a resposta foi "Sim", quem tem acesso a estes dados?** – Se no campo “Outro colaborador ou outro setor da organização, tem acesso a estes dados?”, a resposta foi “Sim”, informamos todos os departamentos, pessoas ou terceiros que recebem esta informação;
- **Estes dados são compartilhados?** - Caso, os dados coletados em um setor/departamento, sejam compartilhados com outros setores/departamentos da organização, pessoas ou empresas parceiras, informamos “Sim”. Caso, os dados coletados em um setor/departamento, não sejam compartilhados com ninguém e são utilizados especificamente por um setor/departamento, informamos “Não”;
- **Com quem estes dados são compartilhados?** - Se no campo “Estes dados são compartilhados?”, a resposta seja “Sim”, informamos todos os setores/departamentos, pessoas ou terceiros que recebem esta informação;
- **Apontamento do Consultor** – Após analisar todas as informações contidas nos campos anteriores, o consultor tenha alguma dúvida, será informado neste campo a informação complementar necessárias para a correta análise das informações contidas no relatório;
- **Resposta do Representante da Organização** – Aqui, a Gerente da **C.A.E.L-ME**, responsável pelo preenchimento do relatório, responderá as dúvidas que foram registradas no campo “Apontamento do Consultor”;
- **Dúvidas do Representante da Organização** – Todas as vezes que o representante da organização teve uma dúvida, foi registrado neste campo, para que o consultor tome conhecimento e possa ajudá-lo; e
- **Medida (s) necessária (s) para adequação à LGPD** – Sempre que for identificado uma ação a ser realizada, para atender as necessidades da LGPD, será registrado neste campo. Desta forma, tanto o representante da organização, como todos aqueles que devem ser envolvidos nesta adequação, terão informações detalhadas das atividades a serem desenvolvidas.

Após analisar todas as informações contidas no Data Mapping, sanar todas as dúvidas, iremos iniciar as adaptações que se fizerem necessárias, para adequar a organização a Lei Geral de Proteção de Dados Pessoais. Estas ações, podem ser desde uma simples troca de formulário, até a suspensão de uma atividade que porventura for identificada como fonte de risco para o atendimento da LGPD.

**Nota 2:** O *Data Mapping*, é um relatório que servirá para a primeira fase das implementações necessárias na organização. Após sua análise e a efetiva execução das adaptações encontradas, as informações que nele estiver contida, será base para a realização

do RIPD. Com a implementação do RIPD, não será mais necessário a utilização do Data Mapping.

## 2.4 – Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

Depois de realizarmos todas as adequações necessárias para atender as solicitações da LGPD, será preenchido o Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Onde estará disponível, para todas as partes interessadas, as análises e as tratativas, tomadas pela C.A.E.L-ME, para o efetivo atendimento da LGPD.

Neste relatório, disponibilizaremos as seguintes informações:

- **Descrição do processo** - Qual o processo foi analisado e está sendo controlado pelo sistema interno de atendimento ao LGPD;
- **Setor/Departamento** – Qual o setor/departamento responsável pelo processo identificado no campo “Descrição do processo”;
- **Identificação dos dados** – Quais os dados pessoais, o processo analisado utiliza para desenvolver sua atividade principal;
- **Coleta** – A forma utilizada neste processo, para coletar os dados pessoais;
- **Tratamento** - Descreve o tratamento que ocorre com os dados pessoais coletados;
- **Finalidade do Tratamento** – Informaremos qual o propósito e necessidade para o tratamento do dado pessoal coletado;
- **Transferência de dados para terceiros** – Se estes dados serão fornecidos para empresas terceiras e se eles os utilizaram para alguma finalidade secundária;
- **Identificação de terceiros** – Utilizamos este campo para identificar quem é a parte interessada que compartilhamos os dados pessoais coletados;
- **Temos contratos exigindo que os terceiros atendam a LGPD? Detalhar.** – Todas as vezes que os dados pessoais são compartilhados com terceiros, informamos se há algum contrato firmado entre as partes que exigem o atendimento da LGPD e os detalhes deste contrato;
- **Fluxo de dados** - Descrevemos o fluxo do tratamento dos dados deste processo, desde a coleta até as eventuais transferências para outras áreas de negócio ou para parceiros de negócios/terceiros;
- **Exclusão de dados** – Se em alguma etapa do processo, os dados pessoais coletados forem excluídos, informaremos como funciona o processo de exclusão e a forma de confirmação da exclusão destes dados;
- **Identificação do Risco** – Para um melhor entendimento e uma correta identificação dos riscos apontados pela organização, este campo foi dividido em 03 (três) etapas de análise. São elas:
  - a) **Identificação do Risco** – Identificamos quais riscos ou ameaças que podem impactar a integridade, disponibilidade e a confidencialidade dos dados pessoais tratados e/ou acarretar a violação da Lei Geral de Proteção de Dados Pessoais;
  - b) **Fonte do risco** – Registramos as fontes de Riscos identificadas durante as análises realizadas; e
  - c) **Eventos possivelmente lesivos** – O que pode levar a violação dos dados pessoais e dos direitos dos titulares.
- **Análise de Risco** – Os riscos identificados foram analisados e identificados das seguintes formas:
  - a) **Gravidade (escala de 1 - 5)** – O risco identificado, juntamente com sua fonte e seu evento lesivo informado no campo “Identificação do Risco”, teve sua gravidade classificada em uma escala de 1 a 5. Onde o nº 1, representa que a sua gravidade é muito pouca e o nº 5, representa que a sua gravidade é muito alta;

- b) **Probabilidade (escala de 1 - 5)** – O risco identificado, juntamente com sua fonte e seu evento lesivo informado no campo “Identificação do Risco”, teve sua probabilidade de acontecer classificada em uma escala de 1 a 5. Onde o nº 1, representa que a sua probabilidade de acontecer é muito pouca e o nº 5, representa que a sua probabilidade de acontecer é muito alta;
  - c) **Risco Total** – O risco total é a multiplicação da escala informada no campo “Gravidade” com a escala informada no campo “Probabilidade”. Desta forma, quanto maior o resultado, maior o risco de que possa acontecer algo que acarrete a violação da LGPD; e
  - d) **Atuar ou aceitar?** - Utilizando como base o resultado apontado no campo “Risco Total”, a organização informará se irá aceitar ou atuar sobre o risco apontado.
- **Como Iremos Atuar nos Riscos Analisados** – Após analisarmos cada risco identificado, informamos no campo “Atuar ou Aceitar?” qual será a forma de atuação da organização. Assim, utilizaremos os campos a seguir para informar os detalhes desta situação:
- a) **Em caso de atuação, quais os controles serão realizados? Em caso de aceite, quais os motivos?** – Independentemente da escolha da organização (Atuar ou Aceitar), este campo será utilizado para explicar o motivo do aceite ou a forma de atuação para minimizar ainda mais o risco identificado; e
  - b) **Há riscos residuais? Quais?** – Após as análises anteriores, informaremos quais os riscos residuais identificados e como iremos monitorá-los.

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD), será o anexo II do Procedimento de LGPD e estará disponível para todas as partes interessadas sempre que necessários e sua atualização será constante, pois os itens controlados por ele, podem ter alterações em todos os momentos e em cada nova reformulação das áreas da organização.

### 3 – Condição da Organização

Com todos os detalhamentos elaborados, onde identificamos em cada setor/departamento, quais as situações que tinham dados pessoais coletados e as formas que estes dados são tratados, identificamos que condição da organização **C.A.E.L-ME** perante a LGPD é de **CONTROLADORA** (Informar se é Controladora ou Operadora) dos dados pessoais coletados e tratados.

### 4 – Regime de Funcionamento

Após realizarmos todas as análises informadas no item 2.3 deste procedimento, a **C.A.E.L-ME**, efetuou as seguintes medidas em atendimento as exigências da LGPD:

- Implementou o “TERMO DE CONSENTIMENTO PARA TRATAMENTO DE DADOS PESSOAIS” nos setores necessários, a fim de informar as partes interessadas a respeito das informações coletas;
- Revisou as formas de atuação junto a cada parte interessada, incluindo, onde necessário, cláusulas em contratos que obriguem a todos a cumprirem as tratativas voltadas para o atendimento da LGPD;
- Implementamos o “TERMO DE COMPROMETIMENTO” onde informamos os critérios e as obrigatoriedades para o atendimento e, principalmente, para o conhecimento de todos os nossos colaboradores, a respeito das exigências da LGPD; e
- Efetuou um treinamento, com todos os nossos colaboradores, no intuito de instruir e dar conhecimento a respeito da LGPD, tanto para as atividades desenvolvidas na organização, quanto em suas vidas pessoais.

No item 2.4 deste procedimento, esclarecemos o RIPD e todas as informações nele contido. Este documento, será a base legal para todas as nossas tratativas e a nossa forma de atuação junto as exigências da LGPD.

## 5 – Reclamações e Petições dos Titulares do Dados

Para atendermos ao artigo 9º da Lei 13709/2018, a **C.A.E.L-ME** disponibilizará um canal de acesso, através do nosso site: [www.csacademia.com.br](http://www.csacademia.com.br)

Este canal está disponível e deverá ser preenchido pelo titular dos dados, sempre que tiver o interesse em saber :

- A finalidade específica do tratamento;
- A forma e a duração do tratamento, observados os segredos comercial e industrial;
- A identificação do controlador;
- As informações de contato do controlador;
- As informações acerca do uso compartilhado de dados e a sua finalidade;
- As responsabilidades dos agentes que realizarão o tratamento; e
- Os seus direitos, com menção explícita aos direitos contidos no art. 18 da Lei 13709/2018.

Ao recebermos sua solicitação, nossa Gerente Carina do Carmo, que é a DPO da organização, terá o prazo médio de 15 (quinze) dias para responder todas as informações solicitadas.

## 6 – Normas de Segurança e Padrões Técnicos

Com a implementação das adequações de atendimento a LGPD, podemos registrar que as nossas normas de segurança e nossos padrões técnicos são:

- **Documentos Físicos:** Após atender a sua necessidade, todos os documentos físicos são arquivados em local protegido (trancados), com acesso limitado a alta direção da **C.A.E.L-ME**.
- **Documentos e Informações Digitais:** Nossos equipamentos são protegidos das seguintes formas:
  - **E-mail:** Proteção total disponibilizado pelo nosso provedor google. Onde ao enviarmos uma mensagem, ela é criptografada e só será aberta quando o destinatário acessar a sua caixa de entrada, utilizando-se de sua senha de acesso;
  - **Banco de dados:** Proteção de acesso do Sistema SCA (Login e senha individual), anti-virus McAfee Security Scan Plus (Sempre na versão mais atual); e
  - **Backup (Cópia de Segurança):** Elaborado toda semana através de HD externo.

## 7 – Obrigações Específicas dos Envolvidos no Tratamento

A **C.A.E.L-ME** determina que a Gerente é a responsável por manter as adequações de atendimento a LGPD sempre atualizada e, principalmente, atuante em toda a organização.

Para isto, após as adequações necessárias para atender a LGPD, no mínimo uma vez a cada 6 meses e, quando necessário, discussões de temas relevante para a continuidade objetiva das implementações realizadas.

Cada colaborador, tem a responsabilidade de manter o seu setor/departamento e, as atividades desempenhadas por ele, atualizadas com as obrigações da LGPD e, sempre que necessário, terá que se reunir com Gerente, para solicitar atualizações específicas para manter sempre atualizado o controle e tratamento dos dados pessoais.

Sempre que possível, ou no mínimo uma vez por ano, deverá ser promovido um treinamento voltado para a atualização e conhecimento de toda a equipe da **C.A.E.L-ME**. Este treinamento, terá a obrigação de manter todos atualizados e sempre atentos a todas as tratativas realizadas pela organização.

O DPO, que também será a Gerente, deverá sempre que necessário, se reunir com todos os colaboradores, para atualizá-los sobre as alterações que porventura acontecer no tratamento dos dados e suas consequências.

Por outro lado, a **C.A.E.L-ME** se coloca a disposição para sempre manter e implementar as mais novas tecnologias digitais de segurança, deixando todas as suas informações digitais protegidas e seguras. Buscando sempre que necessário, impedir ou minimizar a possível propagação indevida dos dados pessoais tratados.

## **8 – Mecanismos de Supervisão e de Mitigação de Riscos**

A **C.A.E.L-ME** determina e nomeia a gerente da organização, a Sra. Carina do Carmo a DPO da organização e, estabelece, que ela irá realizar uma supervisão direta de todas as ações adotadas pela organização, buscando, sempre que necessário, evitar e minimizar possíveis riscos que impliquem em não cumprirmos as exigências da L.G.P.D.

Para isto, ela terá total liberdade de buscar e implementar sistemas de monitoramento e proteções para sempre mantermos um sistema de proteção robusto e com o mínimo de possibilidades de falhas.

Desta forma, entendemos que mitigaremos os riscos, desde o momento de identificar um potencial risco e/ou ameaça, tomando decisões para evitar que ele aconteça ou, no mínimo, minimizar seus impactos em nossas operações e, principalmente, as partes interessadas.