



*ORIENTAÇÕES
GERAIS sobre
**PROTEÇÃO
DE DADOS***



SUMÁRIO

O COMITÊ OLÍMPICO BRASILEIRO E A LEI GERAL DE PROTEÇÃO DE DADOS

1. Você precisa saber por que essa lei foi criada e por que ela é importante. **6**
2. Você precisa saber em que situações ela se aplica e em quais ela não se aplica. **7**
3. Você precisa saber as palavras e expressões da lei para falar sobre proteção de dados. **8**
4. E falando em DPO, é importante você conhecê-lo! **10**
5. Você precisa saber que regras básicas ela coloca para qualquer um que queira tratar dados pessoais. **11**
6. Você precisa saber que direitos ela cria para os titulares de dados pessoais. **14**
7. Você precisa saber o que é um incidente de segurança e como lidar com eles. **15**
8. Por último, você precisa saber que estar adequado à LGPD é um processo contínuo. **16**
 - Novos Projetos e Atividades do COB **18**
 - Aditivos Contratuais **18**
 - Relatório de Impacto à Proteção de Dados Pessoais **19**

Prezados colaboradores e colaboradoras,

Esta cartilha faz parte do Programa de Privacidade de Dados do Comitê Olímpico do Brasil, criado para atender os preceitos da Lei Geral de Proteção de Dados, que estabelece as regras para o tratamento de dados pessoais pela iniciativa privada e pelo poder público.

O conhecimento desta cartilha é primordial para os integrantes da nossa instituição para que as adequações necessárias sejam realizadas e todas as normas, cumpridas.

O Programa de Privacidade é liderado pelo Oficial de Proteção de Dados do COB, que está à disposição de todos para orientações e esclarecimentos.

Boa leitura!

*Paulo Wanderley
Presidente do COB*

O COMITÊ OLÍMPICO DO BRASIL E A LEI GERAL DE PROTEÇÃO DE DADOS

O que você precisa saber?

1 | VOCÊ PRECISA SABER POR QUE ESSA LEI FOI CRIADA E POR QUE ELA É IMPORTANTE.

Cada vez mais empresas, grandes e pequenas, desenvolvem seus modelos de negócio ao redor do tratamento de dados pessoais, extraindo informações preciosas para marketing, análise de risco, desenvolvimento de projetos e produtos e muito mais. Esse desenvolvimento traz muitas oportunidades e, também, alguns riscos aos titulares desses dados (os “donos” dessas informações).

A Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, vem para proteger os direitos fundamentais dos cidadãos, colocando-os no centro do controle sobre suas próprias informações e lhes munindo de ferramentas para ver tais direitos garantidos. Mas a lei também tem uma dupla função. Ela vem também para trazer segurança jurídica para as entidades privadas e públicas que querem tratar esses dados.

O COB trata dados pessoais de muitas pessoas, incluindo seus colaboradores, atletas e seus familiares, fornecedores, entre outros, e tem a responsabilidade de fazer isso com segurança e de acordo com essa nova legislação. Cuidar de dados pessoais é cuidar do COB e da nossa sociedade!

2 | VOCÊ PRECISA SABER EM QUE SITUAÇÕES ELA SE APLICA E EM QUAIS ELA NÃO SE APLICA.

As regras da LGPD **NÃO SE APLICAM** quando o tratamento de dados pessoais:

- for realizado por um indivíduo para fins particulares e sem fins econômicos;
- tenha como único objetivo a produção de conteúdo jornalístico, artístico ou acadêmico;
- tenha como único objetivo a segurança pública, a defesa nacional, a segurança do Estado ou as atividades de investigação e repressão a crimes e ilícitos.

Como essa diferenciação se dá na prática?

A lei **NÃO** se aplica quando:

- os dados sendo tratados não forem sobre uma pessoa física e sim sobre uma pessoa jurídica (uma empresa, entidade, organização etc.);
- os dados pessoais estiverem sendo tratados para produzir uma matéria específica para um jornal;
- os dados pessoais estiverem sendo tratados para produzir um artigo científico.

A lei se aplica, **SIM**, quando:

- os dados sendo tratados sejam sobre EIRELIs (Empresa Individual de Responsabilidade Limitada) ou sobre alguns CNPJs, quando estes estiverem ligados diretamente a um indivíduo;
- os dados pessoais estiverem sendo tratados para administrar as assinaturas do público ao serviço do jornal;
- os dados pessoais estiverem sendo tratados para a operação de escolas e universidades, como em matrículas, histórico acadêmico, pagamentos etc.

3 | VOCÊ PRECISA SABER AS PALAVRAS E EXPRESSÕES DA LEI PARA FALAR SOBRE PROTEÇÃO DE DADOS.

- **Dado pessoal:** toda informação que possa identificar direta (por si só) ou indiretamente (se associada a outras informações) pessoas.

Dados pessoais no COB: informações cadastrais, dados de performance, informações para pagamento de funcionários, presença em cursos e eventos, entre outros.

- **Dado pessoal sensível:** dado pessoal relacionado a tópicos que possam causar discriminação.

Dados pessoais sensíveis no COB: dados sobre origem racial ou étnica, dados referentes à saúde ou à vida sexual, dado genético ou biométrico (identificadores físicos como rosto ou impressão digital), exames laboratoriais etc.

- **Tratamento:** toda operação realizada com dados pessoais.
Exemplos: coleta, produção, utilização, acesso, reprodução, compartilhamento, processamento, armazenamento, eliminação, avaliação da informação, modificação, transferência, difusão ou extração.
- **Titular:** pessoa física a quem se referem os dados pessoais que estão sendo tratados.

Entenda: endereço de e-mail é um dado pessoal – o titular é a pessoa que usa o endereço de e-mail. O número de CPF é um dado pessoal – o titular é a pessoa a qual esse número está vinculado.

Titulares no COB: atletas e seus familiares, colaboradores COB, visitantes dos centros de treinamento, convidados de eventos, participantes de cursos e palestras, fornecedores, treinadores, entre outros.

- **Dado anonimizado:** dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Quando um dado passa por processo de anonimização ele deixa de ser um dado pessoal.
- **Dado pseudonimizado:** caso a tentativa de anonimização ainda permita a identificação do titular do dado, consideramos o dado pseudonimizado. Isto é: embora mascarado, ainda permite a identificação de seu titular.
- **Controlador:** pessoa física ou jurídica com poder de decisão sobre como o tratamento de dados pessoais será realizado.
Entenda: empresa A empregadora sobre os dados pessoais de seus funcionários; empresa B que oferece serviço via aplicativo sobre os dados pessoais dos usuários.
- **Operador:** pessoa física ou jurídica que realiza o tratamento de dados pessoais em nome do controlador sem ter o poder de tomar decisões sobre como esse tratamento será realizado.
Entenda: empresa C terceirizada contratada para executar a folha de pagamento dos funcionários da empresa A; empresa desenvolvedora de software contratada para manutenção do aplicativo oferecido pela empresa B.
- **Agentes de tratamento:** controlador + operador.
- **Encarregado ou Data Protection Officer (DPO):** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. O Encarregado (DPO) ajuda a construir a cultura de conformidade à proteção de dados na empresa.
- **Autoridade Nacional de Proteção de Dados (ANPD):** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

4 | E FALANDO EM DPO, É IMPORTANTE VOCÊ CONHECÊ-LO!

Quem é o DPO do COB?

Ricardo de Simões Nobre. Você pode falar com ele pelo e-mail: ricardo.nobre@cob.org.br ou privacidade@cob.org.br

As principais funções do DPO são:

- orientar os colaboradores do COB sobre o tema da privacidade e proteção de dados pessoais aplicado à realidade da instituição;
- atender ou auxiliar no atendimento aos direitos dos titulares, incluindo responder perguntas e receber reclamações;
- realizar análises de risco sobre as atividades do COB, identificando possíveis desconformidades e sugerindo ajustes;
- fazer a interlocução entre o COB e a Autoridade Nacional de Proteção de Dados, quando necessário;
- liderar ou auxiliar na condução de respostas a incidentes de segurança, orientando os colaboradores do COB e se comunicando com os titulares e a ANPD.

5 | VOCÊ PRECISA SABER AS REGRAS BÁSICAS PARA QUALQUER UM QUE QUEIRA TRATAR DADOS PESSOAIS.

Princípios

A LGPD é baseada em princípios que devem sempre nortear as decisões sobre o tratamento de dados pessoais. Os mais importantes são os princípios da necessidade, finalidade e transparência.

- **Necessidade:** eu realmente preciso de todos esses dados?

O princípio da necessidade propõe a **minimização** do:

VOLUME/QUANTIDADE DE DADOS → Propõe o tratamento da menor quantidade possível de dados. Ou seja, apenas dados indispensáveis para a realização do serviço pretendido devem ser utilizados. A lógica é simples: a atividade pode ser realizada normalmente sem determinado dado pessoal? Se sim, minimize!

TEMPO DE TRATAMENTO → Pressupõe o tratamento dos dados pessoais ou sensíveis pelo menor tempo possível, para alcançar as finalidades que justificaram sua coleta. Em outras palavras, tão logo a finalidade tenha sido alcançada e o dado se torne desnecessário, recomenda-se sua exclusão ou sua anonimização.

- **Finalidade:** por que e para que tratamos esses dados?

Para que um dado seja tratado, é necessário um motivo **concreto** e **específico** que deve ser informado ao titular.

Em outras palavras, a finalidade é o “porquê” por trás de cada atividade. Assim, tudo que se fizer com dados pessoais deve ser baseado em um motivo, e a mera guarda de um dado pessoal sem justificativa já pode trazer riscos para os controladores.

- **Transparência:** o titular dos dados está ciente da necessidade e finalidade do tratamento de seus dados?

No COB, o princípio da transparência é concretizado de várias formas, entre elas por meio do canal de comunicação com os titulares pelo site e por meio dos avisos internos e externos de privacidade.

Além dos 3 principais, também são trazidos pela LGPD os princípios:

- **Qualidade dos dados:** os dados pessoais tratados devem estar sempre corretos, claros, exatos e atualizados.

Responsabilização e prestação de contas: todos os agentes de tratamento dos dados pessoais deverão sempre demonstrar todas as medidas que estão sendo implementadas para o fiel cumprimento da LGPD e seu compromisso com a privacidade e, ainda, demonstrar a eficácia de suas medidas.

- **Adequação:** os dados pessoais tratados devem sempre estar adequados aos propósitos e finalidades informados ao titular de tais dados.
- **Prevenção:** o controlador deverá não só se responsabilizar pelos riscos, mas ir além: empenhar todos os esforços para prevenir quaisquer incidentes de segurança da informação. Uma medida do COB que mostra isso é o seu sistema de classificação da informação por nível de confidencialidade nos e-mails!
- **Livre acesso:** as informações sobre o tratamento dos dados pessoais realizado deverão ser de fácil acesso e compreensão, formuladas em linguagem clara e simples.
- **Não discriminação:** o tratamento de dados pessoais realizado não poderá ser feito para fins discriminatórios ilícitos ou abusivos.
- **Segurança:** utilização de medidas técnicas e administrativas suficientes para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de tratamento. No COB, o princípio da segurança pode ser percebido por meio da sua política de segurança da informação, que estabelece regras, métodos e cuidados que evitam incidentes de segurança.

Bases Legais

Além de garantir que apenas os dados necessários e adequados a essa finalidade (ao “porquê”) sejam utilizados, é preciso também garantir que essa finalidade esteja permitida na lei.

A LGPD traz 10 “bons motivos” ou bases legais para a utilização dos dados pessoais e nenhuma se sobrepõe à outra: quaisquer delas podem autorizar a utilização dos dados.

A base legal mais conhecida é o consentimento.

- **Consentimento** é a manifestação de concordância do usuário com o tratamento de seus dados. Essa manifestação precisa ser livre, informada e inequívoca. Essa você já conhece!

Mas consentimento não é tudo! Temos também:

- **execução de contrato;**
- **cumprimento de obrigação legal ou regulatória;**
- **defesa em processo judicial, arbitral ou administrativo;**
- **tutela da saúde (por profissionais da saúde ou entidades sanitárias);**
- **interesse legítimo;**
- **administração pública;**
- **pesquisa;**
- **proteção da vida ou incolumidade física do titular ou de terceiro;**
- **proteção do crédito.**

6 | VOCÊ PRECISA SABER QUE DIREITOS ELA CRIA PARA OS TITULARES DE DADOS PESSOAIS.

- **Não consentir ou revogar consentimento:** os titulares de dados pessoais têm direito a não consentir com o tratamento de seus dados, assim como revogar consentimento previamente concedido;
- **Confirmação de Tratamento e Acesso:** direito a saber se a instituição trata ou não seus dados e, caso positivo, ter acesso a todos os dados que são tratados;
- **Correção e Eliminação:** direito a ter seus dados corrigidos, atualizados ou eliminados;
- **Informação Sobre Compartilhamento:** direito a ser informado sobre que dados foram compartilhados com quais terceiros e de que forma;
- **Requisição de Portabilidade:** os titulares de dados pessoais têm direito a solicitar que seus dados sejam enviados a outras instituições; e
- **Anonimização e Bloqueio:** direito a ter seus dados anonimizados ou bloquear seu tratamento.



Atenção! *Todas as requisições dos titulares de dados baseadas nestes direitos devem ser atendidas gratuitamente em até 15 dias, sempre em formato que facilite a compreensão e o acesso.*

Para exercer esses direitos, os titulares podem:

1. *Enviar um e-mail diretamente para: privacidade@cob.org.br; ou*
2. *Preencher o formulário pelo site do COB*

É IMPRESCINDÍVEL saber também o que fazer para atender esses direitos!

O COB possui um protocolo de atendimento aos direitos dos titulares.

[ACESSE O FORMULÁRIO](#)

[CLIQUE AQUI para conhecê-lo](#)

7 | VOCÊ PRECISA SABER O QUE É UM INCIDENTE DE SEGURANÇA E COMO LIDAR COM ELES.

O que é um incidente de segurança?

Um incidente de segurança é qualquer acesso não autorizado ou situação acidental ou ilícita de destruição, perda, alteração, comunicação ou difusão de dados pessoais.

Exemplos: um e-mail enviado para o destinatário errado contendo dados pessoais, um celular com acesso ao e-mail do COB que tenha sido roubado, um pen drive perdido, uma deleção acidental de um banco de dados, ou, também, uma invasão do sistema do COB por terceiros não autorizados.

Como prevenir incidentes de segurança?

Para prevenir incidentes, é necessário estar atento à Política de Segurança da Informação do COB.

[CLIQUE AQUI para acessá-la](#)

Dentre outros cuidados necessários, recomenda-se:

- trocar de senha regularmente;
- seguir uma política de mesa limpa, não deixando documentos ao alcance de terceiros;
- evitar trocar informações por whatsapp ou outros meios de comunicação não institucionais;
- ter cuidado ao trabalhar em locais públicos quanto ao volume da sua voz ou quem pode ver sua tela;
- ficar atento a e-mails que pareçam phishing ou golpes.

E o que fazer quando ocorrer um incidente?

O COB possui um plano de resposta a incidentes com todas as informações que você precisa saber para lidar com essas situações.

[CLIQUE AQUI para acessá-lo](#)

Sempre que você suspeitar da ocorrência de um incidente, avise a Equipe de TI: ti@cob.org.br

8 | POR ÚLTIMO, VOCÊ PRECISA SABER QUE ESTAR ADEQUADO À LGPD É UM PROCESSO CONTÍNUO.

A adequação à legislação de privacidade e proteção de dados envolve a criação e a manutenção de rotinas de protocolos. São elas:

Registro de Operação de Tratamento de Dados Pessoais (ROPA)

a. Para que serve

O ROPA é o registro de todas as atividades de tratamento de dados pessoais dentro do COB. Ele serve para dar visibilidade para a Diretoria e o DPO sobre todo o fluxo de dados pessoais dentro da instituição, o que ajuda no processo de identificar possíveis riscos e criar soluções para eles. O ROPA também é muito importante para o atendimento de direitos dos titulares, já que pode ser consultado para encontrar todos os dados pessoais que o COB pode ter sobre um titular, onde estão e qual é o tratamento realizado.

b. Responsabilidade

Toda atividade que envolva o tratamento de dados pessoais deve ser documentada por meio de registro das atividades de tratamento de dados pessoais (ROPA). Essa atividade é coordenada pelo DPO e o preenchimento é de responsabilidade de cada área do COB.

c. Atualizações

A atualização do ROPA deve ser feita semestralmente, com o envio do último registro para atualização pelas áreas do COB, que se responsabilizam por deixar as informações registradas atualizadas e verdadeiras. Cabe ao jurídico e ao DPO supervisionar e atender a dúvidas sobre o ROPA, mantendo-o sempre atualizado e indicando, a partir dele, desconformidades das atividades com a legislação de proteção de dados pessoais.

d. Avaliação de riscos

No momento da atualização do ROPA, ou quando for inserida uma nova atividade de tratamento de dados que ofereça um risco maior ao titular, o DPO deverá realizar uma análise de risco e deve objetivamente:

- revisar as bases legais indicadas pelos gestores das áreas; e
- verificar se as atividades de tratamento de dados atendem aos princípios da LGPD.

NOVOS PROJETOS E ATIVIDADES DO COB

a. O que são

Toda vez que o COB criar um novo projeto, iniciativa ou atividade que envolva dados pessoais, essa novidade precisará ser analisada, logo no início, com um olhar de privacidade e proteção de dados. É importante que, a cada nova iniciativa, a organização demonstre que se preocupou com o impacto à proteção de dados pessoais dos titulares envolvidos.

b. Como realizar

A cada novo projeto que inclua o tratamento de dados pessoais, o DPO deve ser envolvido. Possivelmente um questionário para entender se o processo lida com dados pessoais deverá ser preenchido pelo solicitante.

c. A análise

Com o questionário preenchido em mãos, o DPO obterá um score que poderá auxiliá-lo em sua avaliação de risco sobre o novo projeto. Conforme o grau de risco, o novo projeto: (i) poderá seguir livremente; (ii) precisará de validação da Diretoria para seguir.

ADITIVOS CONTRATUAIS

a. Quando são necessários

Sempre que o COB for parte em um contrato que, por seu objeto, crie um fluxo de dados pessoais entre o COB e um terceiro, o contrato deverá ter previsões sobre privacidade e proteção de dados. Essas previsões também são necessárias quando o contrato, apesar de não criar um fluxo de dados, crie situações em que um terceiro terá responsabilidade sobre dados pessoais do COB, como no caso dos colaboradores.

b. Como realizá-los

Para a criação e assinatura de um aditivo contratual, é necessário entrar em contato com a área do jurídico para que essa equipe avalie o contrato vigente e crie o seu aditivo com as cláusulas pertinentes.

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

a. Quando são necessários

Sempre que o risco de uma atividade de tratamento de dados pessoais for alto, especialmente nas hipóteses de atividades de tratamento com base legal no legítimo interesse ou que envolvam dados sensíveis, o responsável pela atividade deve elaborar, em conjunto com o DPO, um Relatório de Impacto à Proteção de Dados Pessoais, a servir como base para a tomada de decisões pelo COB.

b. Como realizá-los

O Relatório de Impacto é um formulário com questões legais e deve ser preenchido com o auxílio de um profissional da privacidade e proteção de dados ou de um advogado. Para isso, é necessário entrar em contato com a área jurídica do COB.

QUER SABER MAIS?

O COB possui treinamentos disponíveis on-line sobre privacidade e proteção de dados! Qualquer dúvida, entre em contato através do e-mail privacidade@cob.org.br



www.cob.org.br

janeiro/2022