POLÍTICA DE TRATAMENTO E PROTEÇÃO DE DADOS PESSOAIS DO SPORT CLUB CORINTHIANS PAULISTA

A LEI

A Lei geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018) dispõe sobre o tratamento de dados pessoais em meios digitais ou físicos realizados por pessoa natural ou por pessoa jurídica, de direito público ou privado, tendo comoobjetivo assegurar a proteção da privacidade dos dados aos titulares e garantir o desenvolvimento tecnológico, econômico e a inovação. A Lei foi aprovada em agosto de 2018 e passou a vigorar a partir de agosto de 2020.

Por força da mencionada legislação é necessário definir os dados que serão tratados, sua finalidade, as hipóteses de compartilhamento, entre outros pontos.

A presente política tem por objetivo padronizar as práticas detratamento e proteção de dados do Sport Club Corinthians Paulista, visando ainda regular, de forma simples, transparente e objetiva o tratamento dos dados pessoais de clientes, funcionários, colaboradores, atletas e associados.

OBJETIVO

A inviolabilidade da intimidade, da vida privada, da honra e da imagem dos indivíduos é um direito fundamental assegurado pela Constituição Federal de 1988. Resultado de uma das dimensões desse direito fundamental, à proteção das pessoas naturais no que diz ao tratamento dos dados de caráter pessoal se consolida como um direito no Brasil, assegurado pela legislação brasileira, especialmente pela Lei 13.709/2018 (Lei Geral de Proteção de Dados - "Lei Geral de Proteção de Dados").

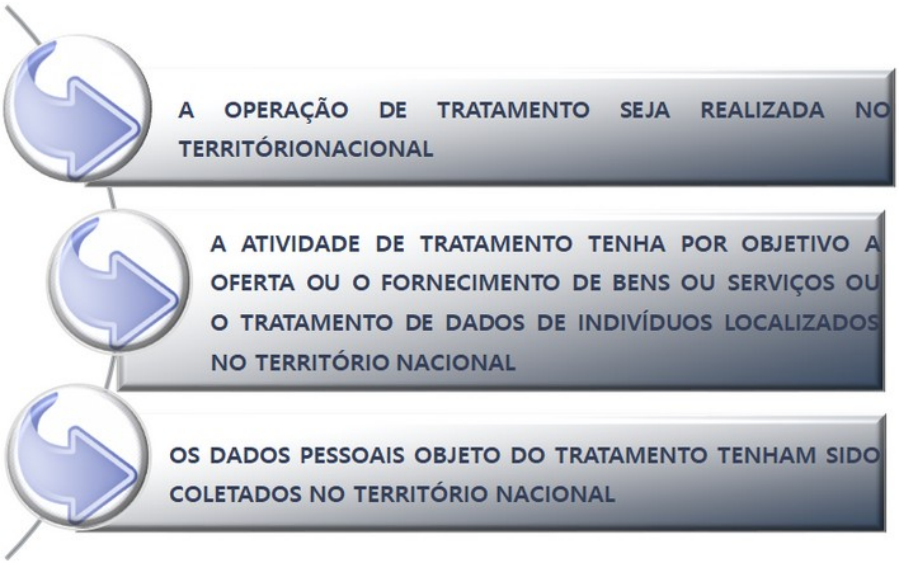
A Lei Geral de Proteção de Dados estabelece regras e princípios para o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. A Lei Geral de Proteção de Dados define que que a proteção de dados pessoais no Brasil tem como fundamentos:

As empresas alinhadas com a responsabilidade social reconhecem o valor da privacidade e da proteção de dados como bem comum e boas práticas de negócios e deste modo, promovem a implementação sistematicamente da Lei Geral de Proteção de Dados e da regulamentação aplicável. A presente Política aplica-se ao Sport Club Corinthians Paulista de acordo com as leis, regulamentos e normas de governança aplicáveis, que, em qualquer caso, prevalecem sobre as disposições contidas neste documento.

- O respeito à privacidade à autodeterminação informativa;
- A liberdade de expressão, de informação, de comunicação e de opinião;
- A inviolabilidade da intimidade, da honra e da imagem;
- O desenvolvimento econômico, tecnológico e a inovação;
- A livre iniciativa, a livre concorrência e a defesa do consumidor;
- Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Escopo de aplicação

No que diz respeito ao escopo de aplicação, o art. 3º estabelece que a Lei Geral de Proteção de Dados se aplica a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:



PRINCÍPIOS DA LGPD

Para contextualizar a Política de Tratamento de Proteção de Dados é necessário compreender, de início, quais princípios regem a legislação.

1. Princípio da Adequação
   Está previsto no inciso II, do artigo 6.º da LGPD e prevê a "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento". Os dados devem ser tratados de acordo com a sua destinação. A coleta de dados deverá ser compatível com a atividade fim do tratamento.

2. Princípio da Necessidade
   A coleta de dados deve ocorrer de forma restritiva, cuidando para que o tratamento dos dados pessoais esteja restrito à finalidade pretendida.

3. Princípio da Transparência
   Visa garantir aos titulares, informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento dos dados.

4. Princípio do Livre Acesso
   Possibilitar que o titular dos dados consulte livremente, de forma facilitada e gratuita, aforma e a duração do tratamento dos dados, bem como sobre a integralidade deles.

5. Princípio da Qualidade de Dados
   Este princípio busca garantir aos titulares dos dados a exatidão, a clareza, a relevânciae a atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

6. Princípio da Segurança
   Compreende medidas técnicas e administrativas para proteger os dados de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração,comunicação ou difusão.

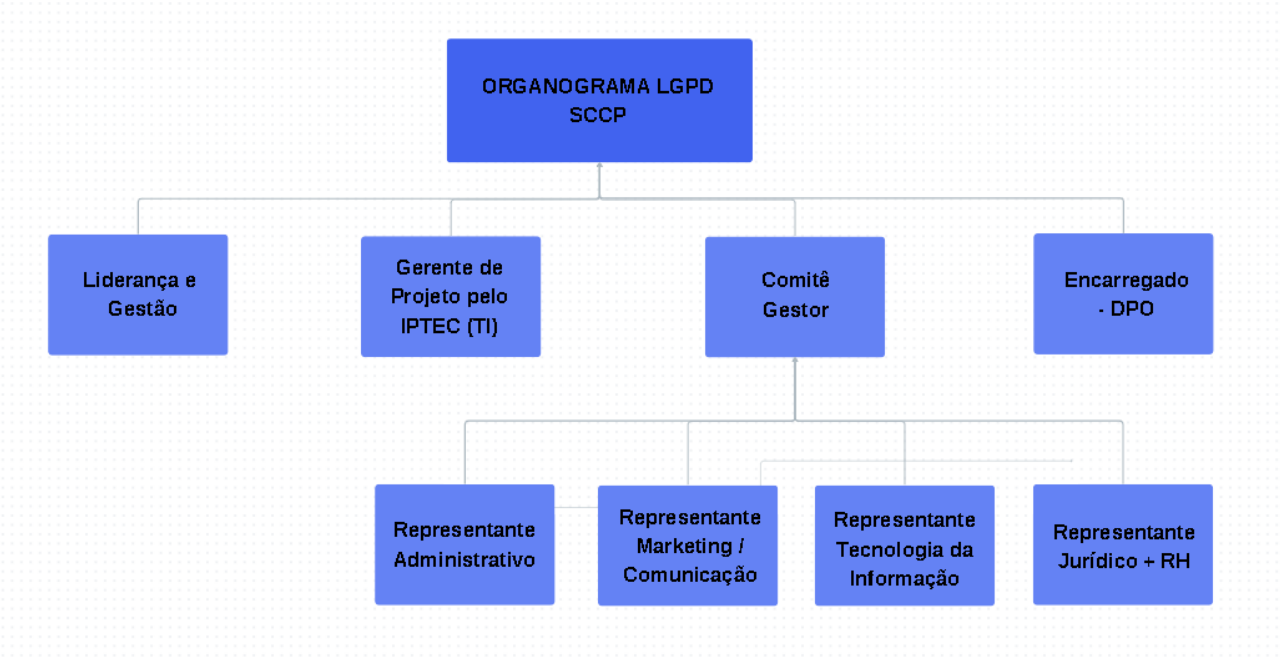
7. Princípio da Prevenção
   É um dos pilares da Segurança da Informação, buscando a antecipação de eventualidades, com a adoção de medidas para prevenir a ocorrência de danos em razão do tratamento de dados pessoais.

8. Princípio da Responsabilidade e Prestação de Contas
   Neste princípio espera-se que o controlador ou o operador demonstrem todas as medidas eficazes e capazes de comprovar o cumprimento da lei e a eficácia das medidas aplicadas.

9. Princípio da Não Discriminação
   O tratamento dos dados não pode ser realizado para fins discriminatórios, ilícitos ou abusivos, ou seja, não se pode excluir de titulares de dados pessoais, no momento de seutratamento, informações determinadas por características, sejam elas de origem racialou étnica, opinião política, religião ou convicções, geolocalização, filiação sindical, estado genético ou de saúde ou orientação sexual.

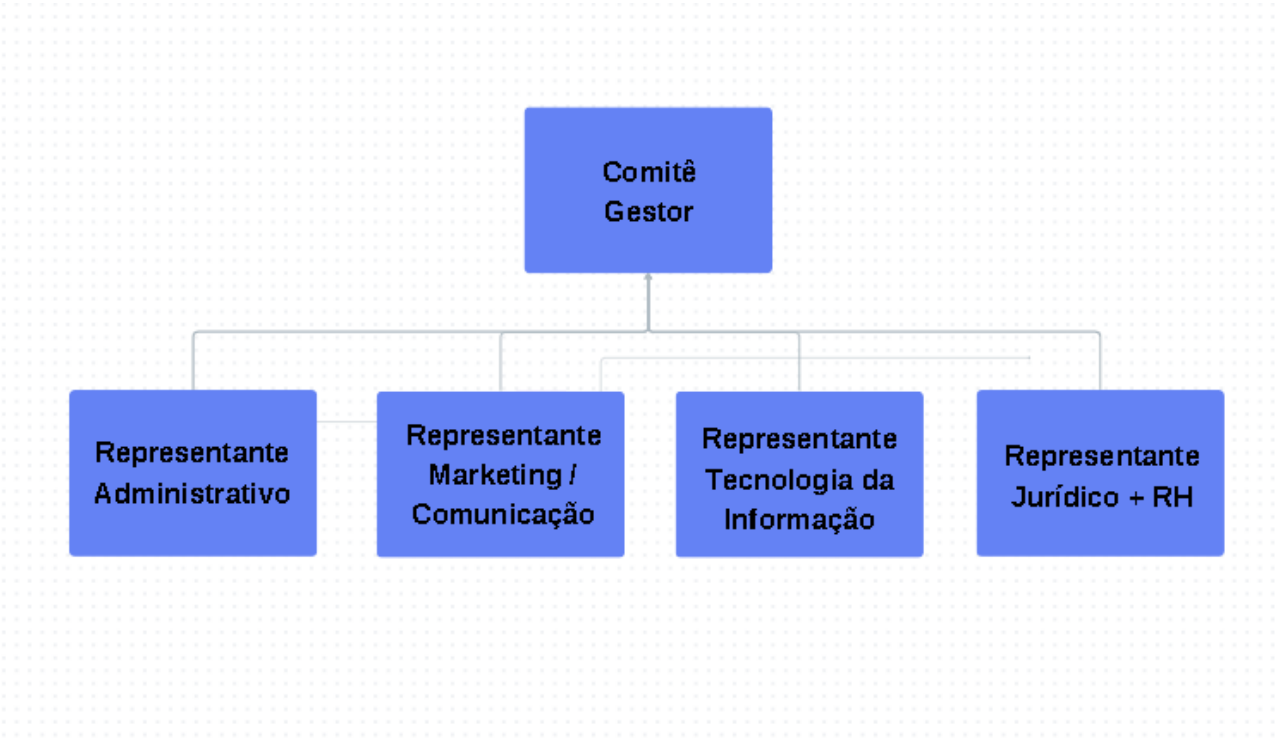
10. Princípio da Finalidade
    Previsto no inciso I do art. 6.º da LGPD, emprega-se como a “realização do tratamentopara propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”, ou seja, o dado deverá, na coleta, ter a indicação clara e completa que a justifique.

RESPONSÁVEL PELO PROJETO



COMITÊ GESTOR

Para a implementação do programa de conformidade com a LGPD foi formado um comitê gestor composto pelos sócios do escritório. O Comité escolhido será o comitê tanto para implantação quanto para a gestão das práticas de tratamento, proteção e segurança dos dados.



PRIVACY BY DESIGN
PRIVACY BY DEFAULT

Significa que as empresas devem colocar em prática medidas técnicas e organizacionais adequadas para garantir, e poder demonstrar, que qualquer tratamento de dados pessoais é desenvolvido considerando todos os requerimentos aplicáveis à proteção de dados pessoais. Estas medidas devem considerar o estado da arte, o custo de implementação e a natureza, o escopo, contexto e finalidades do tratamento, bem como a probabilidade e a gravidade do risco para os direitos e liberdades do Titular em virtude do tratamento ("Privacy by Design").

O controlador deve assegurar que, por padrão (By Default), apenas dados pessoais que sejam necessários para cada finalidade específica de tratamento sejam processados ("Privacy by Default"). Esta obrigação aplica-se ao total de dados pessoais coletados, a extensão de seu tratamento, o período de seu armazenamento e a sua acessibilidade. Em particular, tais medidas devem assegurar, por padrão ("By Default"), que os dados pessoais não sejam acessíveis a um número indefinido de pessoas naturais sem a intervenção individual de um responsável.

O mecanismo de certificação ou a adesão a códigos de conduta podem ser utilizados para tal fim, como elementos para demonstrar a conformidade da Lei Geral de Proteção de Dados nesse ponto. Essas medidas são revistas e atualizadas se necessário, considerando-se a evolução das melhores práticas.

CONSENTIMENTO

O consentimento deve ser dado por um claro ato afirmativo estabelecendo uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada, o que pode ocorrer por uma declaração escrita ou oral, incluindo por meios eletrônicos, sempre mediante comprovação pelo controlador.

O consentimento deve ser aplicado a todas as atividades de tratamento realizadas para a mesma finalidade. Se o tratamento tiver mais de uma finalidade, o consentimento deve ser fornecido para cada uma dessas finalidades, por exemplo, em caixas separadas, caso necessário, pois o tratamento de dados, a depender da finalidade, pode ou não demandar consentimento. Conforme o § 2º do Art.9 da Lei Geral de Proteção de Dados, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

O controlador e o operador são responsáveis por coletar legalmente o consentimento do titular e têm a obrigação de demonstrar perante a Autoridade Nacional de Proteção de Dados (ANPD), que a coleta de consentimento foi realizada legalmente e em total respeito aos regulamentos de privacidade e à Lei Geral de Proteção de Dados.

Cabe ao Controlador provar que o consentimento válido foi obtido do titular. A Lei Geral de Proteção de Dados não prescreve exatamente como isso deve ser feito, no entanto, o Controlador deve ser capaz de provar que um titular em um determinado caso consentiu. Enquanto durar uma atividade de tratamento baseada no consentimento do titular, a obrigação de demonstrar esse consentimento existe. Após o término da atividade de Tratamento, a prova de consentimento deve ser mantida pelo tempo estritamente necessário para o cumprimento de uma obrigação legal ou para que o Estabelecimento possa exercer seus direitos ou defendê-los em demandas legais.

TRATAMENTO DE DADOS

A LGPD se aplica aos casos de tratamento de dados pessoais. Mas, quais atividade englobariam o tratamento de dados?

- Acesso - Possibilidade de comunicar-se com um dispositivo, meio de armazenamento, unidade de rede, memória, registro, arquivo etc., visando receber, fornecer, ou eliminar dados.
- Armazenamento - Ação ou resultado de manter ou conservar em repositório um dado.
- Arquivamento - Ato ou efeito de manter registrado um dado embora já tenha perdido a validade ou esgotada a sua vigência.
- Avaliação - Ato ou efeito de calcular valor sobre um ou mais dados.
- Classificação - Maneira de ordenar os dados conforme algum critério estabelecido.
- Coleta - Recolhimento de dados com finalidade específica.
- Comunicação - Transmitir informações pertinentes a políticas de ação sobre os dados.
- Controle - Ação ou poder de regular, determinar ou monitorar as ações sobre o dado.
- Difusão - Ato ou efeito de divulgação, propagação, multiplicação dos dados.
- Distribuição - Ato ou efeito de dispor de dados de acordo com algum critério estabelecido.
- Eliminação - Ato ou efeito de excluir ou destruir dado do repositório.
- Extração - Ato de copiar ou retirar dados do repositório em que se encontrava.
- Modificação - Ato ou efeito de alteração do dado.
- Processamento - Ato ou efeito de processar dados.
- Produção - Criação de bens e de serviços a partir do tratamento de dados.
- Recepção - Ato de receber os dados ao final da transmissão.
- Reprodução - Cópia de dado preexistente obtido por meio de qualquer processo.
- Transferência - Mudança de dados de uma área de armazenamento para outra, ou para terceiro.
- Transmissão - Movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos etc.
- Utilização - Ato ou efeito do aproveitamento dos dados.

DIREITO DOS TITULARES

O Controlador tem o dever de consultar e atender às instruções detalhadas contidas na Lei Geral de Proteção de Dados e aquelas que venham a ser emitidas pela Autoridade Nacional, que sejam relacionadas ao papel do Controlador no que diz respeito aos direitos dos Titulares.

O Direito à Privacidade e à Proteção de Dados Pessoais deve ser visto à luz da sua função social e deve ser considerado face a outros direitos fundamentais, de acordo com o princípio da proporcionalidade. Apresentar uma reclamação ou o exercício do direito deve estar no centro das operações do Controlador que trata Dados Pessoais ou Dados Sensíveis, independentemente do tamanho da operação de Tratamento.

Procedimentos para exercício dos direitos e reclamações de partes interessadas

Alguns dos procedimentos para o exercício de todos os direitos são estabelecidos pela Lei Geral de Proteção de Dados. O prazo para uma resposta ao pedido do Titular do Dado é, para todos os direitos, imediato para respostas em formato simplificado; ou no prazo de até 15 (quinze) dias, contado da data do requerimento do titular, em caso de requerimento pertinente, cuja resposta deve ser clara e completa que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida em formato gratuito e de sua escolha.

A resposta ao pedido do Titular deve ser por escrito ou por meio de ferramentas eletrônicas, e deve ser clara, concisa e transparente. O Controlador tem o ônus de provar o pedido manifestamente excessivo ou não fundamentado. O exercício de direitos é realizado de forma gratuita ao Titular.

Tempo de Retenção

- O período dos dados armazenamento nem sempre é estabelecido em Lei;
- Se o Controlador decidir por um período mais longo de tempo de retenção do que o previsto em lei, deverá ser registrado propriamente no Registro de Dados;
- Nos casos em que a lei não forneça prazo mínimo para retenção, o Controlador deverá estar apto para justificar o período de retenção de acordo com os Princípios de Responsabilização e Prestação de Contas, Prazo de Prescrição, Necessidade e Adequação.

Direito de Confirmação e de Direito de acesso

A Parte Interessada tem o direito de ser informada de que um tratamento de dados relativo aos seus próprios dados está em andamento e, em caso de resposta afirmativa, obter acesso aos seus Dados Pessoais e receber uma cópia destes.

A confirmação de existência ou o acesso a Dados Pessoais serão providenciados em formato simplificado, imediatamente ou dentro prazo de até 15 (quinze) dias.

Os Dados Pessoais serão armazenados em formato que favoreça o exercício do direito de acesso. As informações e os Dados Pessoais poderão ser fornecidos, a critério do Titular: por meio eletrônico, seguro e idôneo para esse fim ou sob forma impressa. A cópia dos Dados Pessoais é gratuita.

Direito de Correção

A parte interessada tem o direito de obter do Controlador a correção de Dados Pessoais que lhe dizem respeito e que que estejam incompletos, inexatos ou desatualizados.

Direito de Revogação do Consentimento e Direito de Eliminação do Dado Pessoal:

a) A parte interessada tem o direito de revogar o consentimento anteriormente manifestado a qualquer momento mediante manifestação expressa, por procedimento gratuito e facilitado.
b) A parte interessada também tem o direito de obter a eliminação dos Dados Pessoais tratados com o consentimento do Titular.
c) O Controlador deve eliminá-los considerando a tecnologia disponível e os custos de implementação adotando medidas apropriadas.
d) Devem ser deletados quaisquer links, cópias ou reproduções de seus Dados Pessoais.

RETENÇÃO E DESCARTE

Esta Política define os períodos de retenção necessários para todas as categorias específicas de dados pessoais e define os padrões mínimos a serem aplicados ao eliminar certas informações dentro do Sport Club Corinthians Paulista.

A Política de Retenção de Dados visa: i) proteger a integridade e disponibilidade de informações estratégicas; ii) buscar a conformidade com as regulações existentes que requerem a retenção de certos dados pessoais por períodos determinados; iii) buscar a conformidade com a legislação de proteção de dados pessoais quanto à deleção de dados pessoais; iv) melhorar a eficiência e a agilidade de acesso a informações estratégicas; v) reduzir o volume de informações desnecessariamente mantidas; vi) reduzir custos associados com o armazenamento de dados através dos sistemas; vii) facilitar o atendimento de requisições de acesso a informações; e, viii) preservar registros e informações de valor histórico para o Sport Club Corinthians Paulista.

Esta política aplica-se a todos os associados, membros, prestadores de serviço, atletas, sócios, consultores ou prestadores de serviços do Sport Club Corinthians Paulista que possam recolher, processar ou ter acesso a dados.

PRINCÍPIOS E REGRAS DA RETENÇÃO DE DADOS

A retenção de dados pelo Sport Club Corinthians Paulista é orientada pela boa-fé e pelos princípios de proteção de dados pessoais trazidos pela Lei Geral de Proteção de Dados, especialmente os princípios da: i) necessidade, que preconiza a limitação do tratamento ao mínimo para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades das atividades de tratamento de dados; ii) qualidade dos dados, que assegura aos titulares a exatidão, clareza, relevância e atualização dos seus dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; iii) segurança, que exige a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; iv) prevenção, que requer a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; e, v) responsabilização e prestação de contas, que impõe a demonstração, pel Sport Club Corinhtians Paulista, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, bem como da própria eficácia destas medidas, sem prejuízo dos demais princípios aplicáveis.

Considerada a manutenção dos dados pelo exato tempo necessário ao cumprimento das finalidades pretendidas, com as atividades de tratamento de dados pessoais, a retenção de dados pessoais pelo Sport Club Corinthians Paulista observará as seguintes diretrizes.

Os períodos de retenção podem variar conforme a espécie do dado pessoal tratado, a finalidade do tratamento e eventuais outros fatores, tais como prazo prescricional e a existência de obrigação legal que imponha a manutenção de determinado dado por tempo legalmente previsto.

Na ausência de previsão legal específica, a informação não deverá ser mantida pelo Sport Club Corinthians Paulista. Isso significa que, em princípio, os dados devem ser apagados quando: i) o titular revogar eventuais consentimentos dados para legitimar o tratamento; ii) o contrato, ou qualquer outra base legal prevista no artigo 7º da Lei Geral de Proteção de Dados, que respalda as atividades de tratamento tiver sua vigência terminada; ou, iii) as informações e os dados pessoais se mostrarem desatualizados.

Porém, exceções podem se aplicar quanto ao tratamento para fins históricos, estatísticos ou científicos, preferencialmente por meio da utilização de técnicas de anonimização de dados pessoais.

Ao estabelecer ou modificar os períodos de retenção dos dados pessoais, pelo Sport Club Corinthians Paulista deverá considerar os seguintes aspectos: i) objetivos e obrigações aplicáveis; ii) a espécie do dado envolvido; iii) o propósito vinculado ao tratamento dos dados; iv) a base legal que legitima a atividade de tratamento de dados; e, v) as características dos titulares dos dados.

Os dados não devem ser mantidos por período superior ao estabelecido, a não ser que haja uma expressa requisição chancelada ou diretamente emitida pelo Departamentos Jurídico de Compliance e do DPO pelo Sport Club Corinthians Paulista para tanto.

Para determinar o período de retenção adequado para os dados pessoais, consideramos a quantidade, a natureza e a sensibilidade dos dados pessoais, o risco potencial de danos decorrentes do uso não autorizado ou da divulgação de seus dados pessoais, a finalidade de processamento dos seus dados pessoais e se podemos alcançar tais propósitos através de outros meios, bem como os requisitos legais aplicáveis.

Como o Sport Club Corinthians Paulista protege suas Informações de Dados Pessoais:

O Sport Club Corinthians Paulistas emprega medidas técnicas de segurança e organizacionais para proteger suas informações e seus dados pessoais. Os dados serão armazenados em um ambiente operacional seguro que não é acessível ao público.

O Sport Club Corinthians Paulista se esforça para proteger a privacidade dos dados pessoais e demais informações que são armazenadas, contudo não se pode garantir total segurança.

Consequentemente, o Sport Club Corinthians Paulista, suas empresas parceiras e afins, terceiros, provedores de serviços e seus respectivos escritórios, sócios, empregados, associados, atletas e prestadores de serviço não representam, autorizam ou garantem que informações pessoais estarão protegidas contra invasão de "hackers" ou qualquer outra forma ou dispositivo desautorizado no ambiente da internet.

Por isso, caso o Usuário identifique ou tome conhecimento de algo que comprometa a segurança dos dados pessoais, o Sport Club Corinthians Paulista pede que entre em contato por meio do e-mail dpo@sccorinthians.com.br ou outra forma de contato que você escolher dentre as disponibilizadas pelo Sport Club Corinthians Paulista para este fim.

De toda sorte, o Sport Club Corinthians Paulista, para se resguardar e proteger seus direitos, poderá acessar, ler, preservar e fornecer quaisquer dados e informações sobre o Usuário, incluindo interações suas, caso sejam necessários para:

- Cumprimento de obrigação legal, ordem judicial ou requisição de autoridades administrativas que detenham a devida competência para tanto;
- Cumprir ou aplicar outros Acordos e/ou Contratos; e,
- Proteger os direitos, propriedade e segurança do Sport Club Corinhtians Paulista, bem como de nossos colaboradores, associados, atletas, prestadores de serviços e/ou outro Usuário.

Por Quanto tempo os Dados Serão Armazenados?

O Sport Club Corinthians Paulista manterá os dados pessoais do Usuário do Site somente pelo tempo que for necessário para cumprir com as finalidades para as quais os coletamos, inclusive para fins de cumprimento de quaisquer obrigações legais, contratuais, de prestação de contas ou requisição de autoridades competentes.

Todos os dados coletados serão excluídos de nossos servidores quando o Usuário assim requisitar, salvo se houver qualquer outra razão para a sua manutenção, como eventual obrigação legal de retenção de dados, ou necessidade de preservação destes para resguardo de direitos da Sport Club Corinthians Paulista.

MEDIDAS RECOMENDÁVEIS

1. Elaborar norma interna aos funcionários e colaboradores determinando a obrigação de bloquear automaticamente a tela do notebook ou do computador após um período determinado de não uso da máquina.

2. No caso de utilização de serviços em nuvem ou VPN, é recomendável que o departamento de TI configure o monitoramento dos dispositivos, incluindo verificações de invasão de dispositivos ou bloqueando as informações para que elas não possam ser salvas da nuvem para a “unidade local C”.

3. Adotar medidas de segurança com relação a senhas e acessos a fim de minorar os riscos e possíveis danos aos titulares de dados, no tocante à maior fragilidade quanto ao aspecto da segurança do Wi-Fi doméstico, possibilitando um risco maior de violações como o roubo de credenciais e senhas.

4. Estabelecer um plano de proteção para a documentação física e para a documentação digital. A empresa deve realizar uma avaliação para compreender se determinada documentação possui dados sensíveis e elaborar o Relatório de Impacto à Proteção de Dados (DPIA), com previsão do nível de riscos e de quais medidas de segurança poderão ser adotadas.

5. Elaborar um registro acerca dos colaboradores e funcionários que possuem permissão para acesso a documentos, informações e dados pessoais, tanto em suporte físico como digital, e especificar qual seria a forma correta para o transporte dos mesmos, traçando diretrizes para seu acesso limitado aos funcionários e colaboradores estritamente necessários com relação à finalidade do tratamento respectiva.

6. Elaborar treinamentos específicos para os colaboradores e funcionários e promover sua conscientização acerca da importância de proteger a privacidade, as informações e os dados pessoais sob sua responsabilidade, objeto de tratamento de dados, incluindo a elaboração de um plano de ação no caso de incidente de segurança, em especial quanto às normas e demais disposições da Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados), bem como ao modo de se relacionar e realizar o atendimento ao titular dos dados. Outrossim, devem ser realizados treinamentos e medidas de conscientização no tocante à segurança da informação, traçando diretrizes quanto as responsabilidades, padrões de controle de informação e sua relação com a proteção de dados pessoais.

7. Adotar a medida de segurança de criptografia dos dispositivos, em especial quando se tratar de dados sensíveis, e no caso de compartilhamento de dados sensíveis, de preferência adotar-se como regra a anonimização de dados, adotando-se o procedimento mais robusto possível, com observância de técnicas específicas de anonimização de dados de saúde, a fim de evitar incidentes tais como uso indevido dos dados pessoais, vazamento de dados, entre outros.

8. Adotar medidas de segurança visando à proteção do navegador de internet (VPN - Virtual Private Network). Não utilizar Wi-fi público.

9. Elaborar um backup dos dados pessoais objeto de tratamento, garantindo um armazenamento seguro destes.

10. Garantir a utilização pelos colaboradores e funcionários de um antivírus e de um firewall, ambos atualizados, eficazes e de origem lícita. Garantir a utilização de softwares legítimos e seguros pelos funcionários e colaboradores.

11. Prevenir possíveis invasões ou outro incidente de segurança por meio da utilização de um Firewall de Aplicativo da Web (WAF) ou um Sistema de Prevenção de Intrusões (ISP) focado na vulnerabilidade.

12. Recomendar aos funcionários e colaboradores o não empréstimo e compartilhamento de computadores e celulares para terceiros, em especial, para terceiros sem vínculo com a empresa, ou mesmo com conhecidos ou pessoas da família.

13. Recomendar aos funcionários e colaboradores o não acesso de arquivos corporativos em equipamentos desconhecidos e sem proteção, bem como a não proceder ao download de programas ou o acesso de sites não autorizados.

14. Garantir a adoção e implementação de mecanismos de segurança dos dados nos softwares e recursos utilizados, implantando sistemas de monitoramento e controle dos dispositivos, respeitados os direitos dos trabalhadores, isto é, adotando-se medidas de forma proporcional e razoável, bem como amparadas em prévia informação aos colaboradores e funcionários acerca de sua utilização.

15. Fornecer, quando for necessário, os equipamentos e a infraestrutura essenciais para o desempenho seguro das atividades dos colaboradores e funcionários, sob o regime de comodato, ou mediante reembolso dos custos pela empresa, em especial fornecendo as

necessárias proteções tecnológicas eficazes, a fim de evitar vazamento de dados pessoais ou outro incidente. Recomenda-se, de preferência o fornecimento de dispositivos móveis corporativos necessários ao desenvolvimento das atividades dos colaboradores e funcionários, mediante assinatura de um Termo.

16. Criar protocolos para evitar que pessoas não autorizadas acessem a rede interna da organização.

17. Verificar se os contratos societários, de colaboração, de prestação de contas ou de trabalho celebrados com os colaboradores e funcionários possuem previsão do trabalho efetuado na forma de teletrabalho, telecomutação ou home office, e de trabalho remoto, e acrescentar tal previsão em caso de omissão, bem como verificar a existência de cláusula de confidencialidade acerca dos dados pessoais objeto de compartilhamento e tratamento pelos colaboradores e funcionários.

18. Criar padrões específicos para a realização do trabalho, no caso de não utilização de equipamentos corporativos, com a definição de um padrão mínimo de respeito à normas de segurança, normas de proteção de dados e privacidade e comportamentais.

19. Elaborar um conjunto de normas de Acesso Remoto, definindo regras, produtos, ferramentas que devem ser utilizadas em cada tipo de equipamento, quando do acesso remoto.

20. Elaborar um conjunto de normas de uso da Internet, estabelecendo regras básicas, controle e responsabilidades do usuário, em especial quando da utilização de recursos corporativos, bem como no tocante à utilização do serviço de correio eletrônico da organização ou de correio eletrônico particular, utilizando recursos da organização. Da mesma forma devem ser definidas regras, controles e responsabilidades do usuário quando do uso de serviços de Rede Social Pública utilizando recursos da organização ou utilizando recursos particulares.

21. No que se refere às reuniões remotas de trabalho o usuário deve se obrigar a permanecer em local com tranquilidade e sigilo adequado à reunião. Deverá ser utilizada ferramenta de licença corporativa e paga para a realização das reuniões remotas, verificando-se todos os parâmetros de segurança pela Área de Segurança da Informação da organização.

22. Caso seja possível recomenda-se que os colaboradores e funcionários utilizem de um computador próprio para o trabalho e outro para seus assuntos pessoais, de forma a separar e melhor proteger as informações e os dados pessoais.

23. Cada usuário deve ter identificação individual e intransferível.

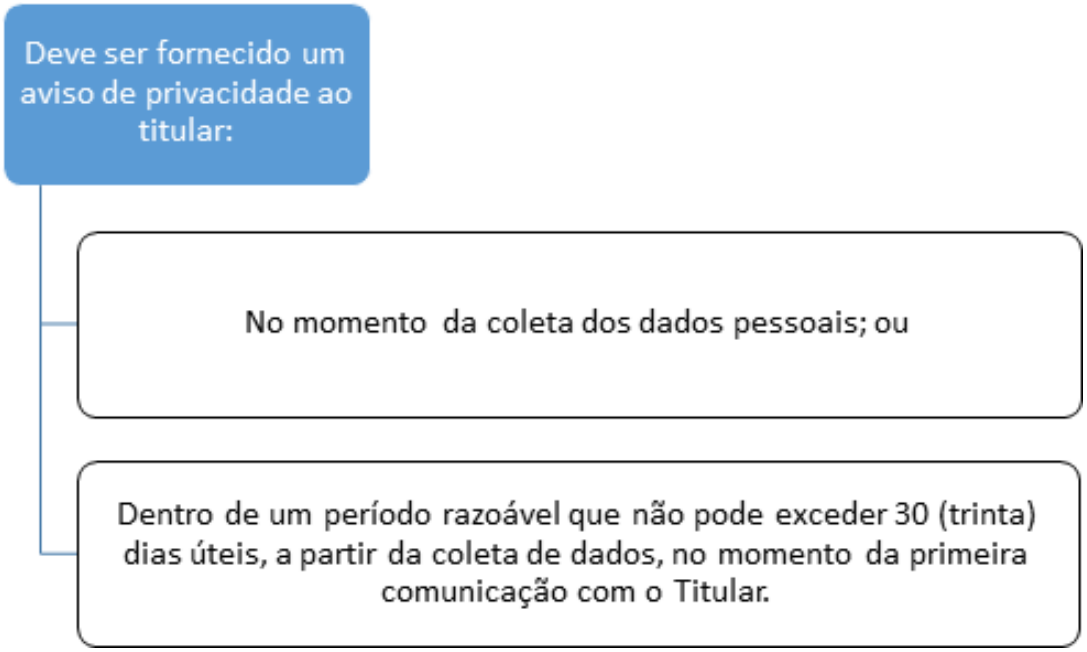
24. Todos os acessos e ações do usuário devem ser registradas.

25. A autenticação deve ser realizada com exigência de dupla autenticação, por um período aproximado de até 4 (quatro) horas de atividade.

AVISO DE PRIVACIDADE

O Aviso de Privacidade deve conter:

- Informações gerais, identificação e de contato do controlador;
- Informações gerais e de contato do Encarregado – DPO;
- Objeto e modalidades do tratamento;
- Finalidade e base legal do tratamento;
- Fonte dos dados pessoais;
- Destinatários com quem os dados pessoais sejam compartilhados;
- Transferência de dados pessoais;
- Responsabilidades dos agentes que realizam o tratamento (Controlador e do Operador);
- O período de armazenamento de dados pessoais;
- Qualquer uso de tomada de decisão automatizada;
- Os direitos dos Titulares e os meios para exercê-los;
- O aviso de privacidade deve ter um texto conciso, claro e inteligível e deve ser facilmente acessível ao Titular;
- A linguagem deve ser clara, simples, e compreensível pelos vários públicos (ex: menores de idade, portadores de necessidades especiais, etc.);
- O Aviso de Privacidade é fornecido, a princípio, por escrito e, de preferência, em formato eletrônico. Deve ser formado por estruturas progressivas, a fim de melhor atender aos múltiplos segmentos de todas as informações necessárias.



REGISTRO DE TRATAMENTO DE DADOS

A Lei Geral de Proteção de Dados prevê que o Controlador e o Operador devem manter registro das operações de tratamento que realizarem.

A finalidade e os objetivos do tratamento devem ser representados no registro do Controlador, enquanto as escolhas operacionais no tratamento devem ser representadas no registro dos Operadores. Os registros do Controlador e dos Operadores podem ser integrados em uma única plataforma eletrônica para garantir o cumprimento da obrigação da Lei Geral de Proteção de Dados, mas é primordial que haja um mapeamento dinâmico do tratamento e seu ciclo de vida. O registro também deve incluir infraestruturas digitais, plataformas, software, aplicativos, etc.

O conteúdo mínimo do registro do Controlador deve apresentar:

- O nome e os dados de contato do Controlador e, quando aplicável, dos Controladores Conjuntos, do representante legal do Controlador e do Encarregado- DPO;
- As finalidades do tratamento;
- Descrição das categorias de Titulares e das categorias de Dados Pessoais;
- As categorias de destinatários para os quais os Dados Pessoais foram ou serão divulgados, incluindo destinatários em terceiros países ou empresas internacionais;
- Quando aplicável, as transferências internacionais de dados pessoais para outro país ou uma organização internacional, incluindo a identificação desse outro país ou organização internacional.
- Sempre que possível, os prazos previstos para o descarte das diferentes categorias de Dados Pessoais;
- Sempre que possível, uma descrição geral das medidas de segurança referidas no Art. 46 da Lei Geral de Proteção de Dados.

PONTOS DE ATENÇÃO

Deve-se ter em mente a necessidade de um monitoramento das práticas diária em prol da segurança cibernética. Assim, merecem atenção redobrada as seguintes hipóteses:

- Perda de confidencialidade dos dados pessoais protegidos pelo sigilo profissional;
- Reversão não autorizada de pseudonimização;
- Qualquer outra desvantagem econômica ou social significativa onde os titulares podem ser privados de seus direitos e liberdades ou impedidos de exercer controle sobre seus dados pessoais;
- Quando são tratados dados pessoais que revelem origem racial ou étnica, opiniões políticas, religiosas, crenças filosóficas ou filiação sindical;
- Quando são tratados dados genéticos, dados relativos à saúde ou dados sobre vida sexual;
- Condenações penais, infrações penais ou a medidas de segurança conexas - onde aspectos pessoais são avaliados. Em em particular para análise e previsões de aspectos relativos ao desempenho no trabalho, situação econômica, saúde, preferências, interesses pessoais, confiabilidade, comportamento, localização ou movimentos, a fim de realizar ou usar o Perfilamento (Profiling);
- Quando são tratados dados pessoais de pessoas naturais vulneráveis (crianças e adolescentes);
- Quando o processamento envolver uma grande quantidade de dados pessoais e afeta um grande número de titulares.

PROBABILIDADE E A GRAVIDADE DO RISCO PARA OS DIREITOS E LIBERDADES DO TITULAR

A probabilidade e a gravidade do risco para os direitos e liberdades do titular devem ser determinadas por referência à natureza, âmbito, contexto e finalidades do tratamento. O risco deve ser avaliado com base em uma avaliação objetiva, através da qual se estabeleçam se as operações de tratamento de dados envolvem um risco ou um alto risco.

Diretrizes na implementação das medidas apropriadas e na demonstração da conformidade

As diretrizes na implementação das medidas apropriadas e na demonstração da conformidade do controlador e do operador, especialmente relacionadas na identificação dos riscos relatados no tratamento, sua avaliação em termos de origem, natureza, probabilidade e gravidade, e a identificação das melhores práticas para mitigar os riscos, podem ser realizadas em particular através de Códigos de Conduta aprovados, certificações aprovadas e diretrizes emitidas pelo Comitê ou indicações emitidas pelo Data Protection Officer. O Comitê poderá ainda emitir diretrizes sobre operações de tratamento que são consideradas improváveis de resultarem em altos grandes riscos à proteção de dados e à vida privada das pessoas naturais e indicar quais medidas podem ser suficientes nestes casos para tratar tais riscos.

Tal como indicado nas orientações do WP 29 Grupo de trabalho das Autoridades de Controle de Proteção de Dados (IAPP), a referência aos "direitos e liberdade dos titulares'' diz respeito principalmente aos seguintes direitos:

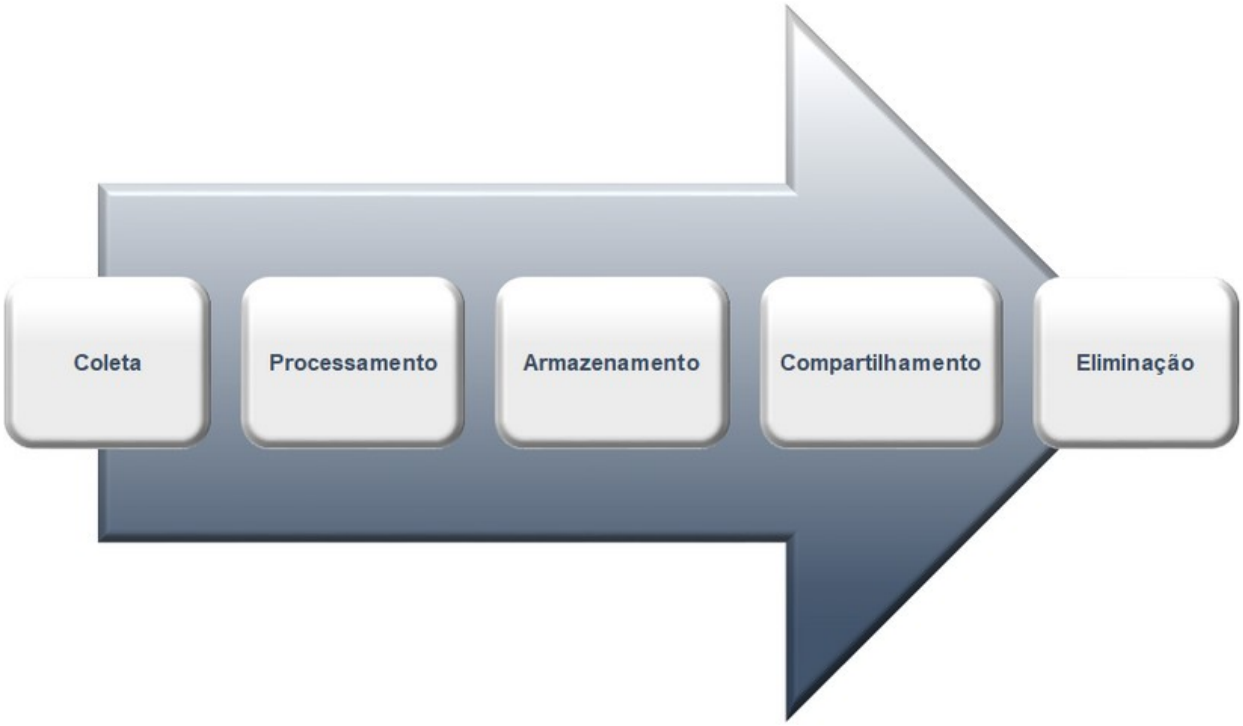
- Avaliação de desempenho, valoração, pontuação;
- Decisões automatizadas que produzem efeitos jurídicos significativos (ex: recrutamento, concessão de empréstimos, cessão de benefícios ao cliente);
- Combinação ou comparação de conjuntos de dados de dois ou mais processos realizados para vários fins e / ou por diferentes Controladores;
- Perfilamento (Profiling) e predição, em especial em consideração dos aspectos relativos a desempenho profissional, situação econômica, saúde, preferências ou interesses pessoais, confiabilidade ou comportamento, localização ou movimentos da pessoa em causa;

- Monitoramento sistemático em grande escala em uma área acessível ao público;
- Dados Pessoais Sensíveis, conforme definido no do Art. 11 da Lei Geral de Proteção de Dados (por exemplo, informações sobre opiniões políticas de pessoas), bem como Dados Pessoais relativos a antecedentes criminais;
- Tratamento de dados em larga escala com o uso da gestão do relacionamento com o cliente, big data, data lake, algoritmos, incluindo o recurso a provedores de nuvem como Operadores;
- Fusão de bases de dados (especialmente para perfis ou outro cruzamento de informações sobre o Titular), embora não prevista no momento da divulgação do consentimento para os vários em processamento;
- Processamento que envolva dados pessoais vulneráveis, como por exemplo: crianças e adolescentes (legalmente considerados incapazes de se opor ou aceitar deliberada e conscientemente o tratamento dos seus dados) - são segmentos da população mais vulnerável que requerem proteção especial e em qualquer caso em que é possível identificar desequilíbrio na relação entre a posição dos dados e o Controlador do processamento como no empregador – relação de emprego;
- Uso de sistemas predictivos através de sistemas analíticos, uso de sistemas para detecção de dados biométricos, processamento que se relacionam com a internet de coisas;
- Quando o próprio processamento impede os Titulares de exercerem um direito ou se beneficiarem de um serviço ou de um contrato.

CICLO DE VIDA DOS DADOS

A descrição do ciclo de vida dos dados deve considerar:

a) A coleta dos dados,
b) A classificação,
c) O estabelecimento;
d) A finalidade do tratamento,
e) As categorias do tratamento;
f) As medidas de segurança,
g) A transferência internacional de dados para outros países;
h) A eliminação;
i) O prazo de conservação de dados pessoais



ENCARREGADO (DATA PROTECTION OFFICER)

O papel do Encarregado (DPO – Data Protection Officer):

A Lei Geral de Proteção de Dados exige que as empresas que realizam o tratamento de dados pessoais nomeiem um Encarregado pelo tratamento de dados pessoais (DPO) que deve exercer as atividades previstas no § 2º do Art. 41 da lei. Além das exigências da Lei Geral de Proteção de Dados acerca do o papel do DPO, para O pelo Sport Club Corinthians Paulistas essa função deverá corresponder adicionalmente às atividades e aos padrões estabelecidos globalmente pela mesma.

O DPO é selecionado considerando sua experiência em privacidade e proteção de dados, suas características profissionais, sua habilidade para cumprir as tarefas que lhe sejam atribuídas;

No desempenho de suas atribuições, o DPO leva em consideração os riscos inerentes ao tratamento, assim como a natureza, o escopo, o contexto e os objetivos do mesmo;

O Controlador e o Operador devem envolver o DPO em todas as questões relativas à proteção de Dados Pessoais e garantir sua independência na execução das funções e do seguinte modo:

Garantir que haja o devido atendimento às reclamações e comunicações dos Titulares, que sejam prestados os esclarecimentos e adotadas as providências necessárias;

Apoiar e aconselhar o controlador, operador, seus representantes legais, gestor do controlador, gerentes de tarefas do controlador e pessoa autorizada a tratar dados pessoais em relação às obrigações decorrentes da legislação e regulamentação de proteção de dados, especialmente em relação à Lei Geral de Proteção de Dados e às normas editadas pela Autoridade Nacional;

Projetar programas de conformidade e monitorar a implementação, definir governança de proteção de dados, avisos de privacidade padrão, cláusulas contratuais padrão e normas corporativas globais.

Apoiar o Controlador e o Operador na negociação de contratos de proteção de dados, definir em conjunto com o Controlador a metodologia DPIA, definir os requisitos da implementação dos direitos dos Titulares;

Definir e implementar planos de treinamento e conscientização de acordo com o Controlador e o Operador;

Fornecer, se necessário, uma opinião sobre a avaliação do impacto na proteção de dados e monitoramento de progresso;

Cooperar e atuar como ponto de referência da Autoridade Nacional, recebendo comunicações e adotando providências;

Atuar como ponto de contato para a Autoridade Nacional para questões relacionadas com o tratamento, incluindo incidentes de dados;

Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais

CONTROLADOR E OPERADOR

O **Controlador** tem o dever de consultar as instruções emitidas pela Autoridade Nacional de Proteção de Dados (ANPD) e também as diretrizes e melhores práticas internacionalmente reconhecidas em matéria de Proteção de Dados Pessoais. As indicações a seguir são exemplificativas e não exaustivas.

- O Controlador define a finalidade e o significado do tratamento do dado pessoal;
- Controladores implementam medidas técnicas e organizacionais apropriadas para assegurar a Proteção dos Dados Pessoais de acordo com a Lei Geral de Proteção de Dados;
- Os Controladores também têm o ônus de provar a conformidade com a Lei Geral de Proteção de Dados;
- Os Controladores respondem na pessoa de seus representantes legais, por cada atividade de tratamento executada, cumprir integralmente as obrigações estabelecidas pela Lei Geral de Proteção de Dados e sua respectiva regulamentação;
- O Controlador que trata dados pessoais deve definir as pessoas autorizadas ao tratamentos dentro de sua empresa;
- O Controlador deve organizar-se internamente para melhor cumprir com as várias obrigações estabelecidas pela Lei Geral de Proteção de Dados e pela presente Política;
- O Controlador é apoiado e aconselhado pelo DPO e da mesma forma, apoia a atividade do DPO.

Com o suporte do DPO, o Controlador deve:

- Planejar e executar as medidas adequadas de segurança, privacy by design e by default, aplicando as melhores práticas e os mais altos padrões de mercado;
- Fornecer a cada ano os recursos adequados para serem dedicados aos objetivos de proteção de dados na operação de negócios e soluções digitais;
- Treinamento contínuo aos seus próprios empregados e terceiros;
- Executar auditorias nos terceiros que tratam os dados em seu nome;
- Cooperar com a Autoridade Nacional de Proteção de Dados (ANPD) nos cursos de suas iniciativas de investigação.

O **Operador** tem o dever de consultar e atender às disposições da Lei Geral de Proteção de Dados e àquelas eventualmente emitidas pela Autoridade Nacional de Proteção de Dados, acerca de suas responsabilidades. As seguintes indicações são exemplificativas não exaustivas.

Os deveres do Operador são regidos por um contrato ou outro ato jurídico sob a Lei Geral de Proteção de Dados ou demais normas sobre proteção de dados pessoais que vincule o Operador às instruções do Controlador e que regule a natureza, a duração e a finalidade do tratamento, o tipo de dados pessoais tratados, as categorias dos titulares, as obrigações e os direitos do Controlador.

O contrato ou outro ato jurídico é definido pelo Controlador junto ao o Operador e deve estabelecer que esse último:

- Trate os Dados Pessoais somente em instruções documentadas do Controlador, incluindo com referência a transferência dos Dados Pessoais a um terceiro país ou organização internacional, a não ser que seja obrigado a fazê-lo pela legislação a qual o Operador esteja submetido; nestes casos o Operador deverá informar ao Controlador todos os requerimentos legais antes do Tratamento, a menos que a lei proíba tais informações em fundamentais relevantes de interesse público;
- Assegure que as pessoas autorizadas a tratar os Dados Pessoais tenham a obrigação contratual ou legal a manter sigilo e confidencialidade;
- Adote todas as medidas de segurança exigidas nos termos do, bem como Art. 46 da Geral de Proteção de Dados;

- Adote, considerando a natureza do tratamento, medidas técnicas e organizacionais apropriadas, na medida do possível, que permitam ao Controlador atender as requisições dos Titulares no exercício de seus direitos, conforme previstos no Capítulo III da Lei Geral de Proteção de Dados;
- Preste assistência ao Controlador para garantir a conformidade com obrigações relacionadas às medidas de Segurança (Capítulo VII da Lei Geral de Proteção de Dados), que são a Notificação e Comunicação de Incidente de Segurança de Dados (Art 48 da Lei Geral de Proteção de Dados), DPIA (Art. 38 da Lei Geral de Proteção de Dados), levando em conta a natureza do tratamento e a informação disponível para o Operador;
- Elimine ou devolva, a critério exclusivo do Controlador, todos os Dados Pessoais ao término da prestação dos serviços relacionados, deletando cópias existentes, a não ser que disposto expressamente em contrário na legislação aplicável para o armazenamento dos Dados Pessoais objeto do respectivo tratamento;
- Disponibilize ao Controlador todas as informações necessárias para demonstrar o cumprimento das obrigações estabelecidas na Lei Geral de Proteção de Dados, bem como permita e contribua para auditorias, incluindo inspeções, conduzidas pelo Controlador ou outro auditor contratado pelo Controlador;
- Os Operadores que subcontratam os serviços de terceiros para a execução do tratamento respondem perante o Controlador quanto a possíveis falhas desses terceiros, bem como se responsabilizam por quaisquer indenizações e/ou compensações por danos causados pelo respectivo tratamento, a menos que provem que o evento danoso não lhe seja atribuível em nenhuma hipótese;
- As autoridades públicas que possam receber comunicação de dados pessoais no contexto de uma investigação específica em conformidade com a lei não serão consideradas destinatários e não devem ser entendidas como Operadores.

MEDIDAS DE SEGURANÇA

O Controlador tem o dever de consultar e atender às disposições contidas na Lei Geral de Proteção de Dados e àquelas que venham a ser emitidas pela Autoridade Nacional acerca das medidas de segurança aplicáveis às atividades de Tratamento. As seguintes indicações são exemplificativas e não exaustivas da complexidade desses temas.

Considerando o estado da arte, os custos de implementação, a natureza, âmbito, contexto e finalidades do tratamento, bem como o risco e impacto perante os direitos e liberdades dos titulares, o Controlador e o Operador devem implementar medidas técnicas e organizacionais destinadas a garantir um nível de segurança adequado, incluindo, entre outras, as medidas de Privacy by Design (Desde a concepção) e Privacy by Default (Por padrão).

O Controlador e o Operador devem:

- Rever e proteger todos os sistemas, identificação de aplicações e infra estruturas e acesso lógico do Sport Club Corinthians Paulista;
- Rever e gerir de forma segura os Dados Pessoais e Sensíveis, com o objetivo de garantir uma elevada qualidade de dados e de forma que o Tratamento se limite ao necessário e ao adequado;
- Segregar os Dados Pessoais e perfilar usuários que lidem com Dados Pessoais, limitando acesso e atribuições de acordo com o estritamente necessário para execução de suas tarefas;
- Pseudonimizar, anonimizar e criptografar Dados Pessoais e Sensíveis;
- Assegurar permanentemente a confidencialidade, integridade, disponibilidade e resistência dos sistemas e serviços de Tratamento;
- Restaurar prontamente o acesso e disponibilidade dos Dados Pessoais em caso de acidente físico ou técnico;
- Testar, verificar e avaliar regularmente a eficácia das medidas técnicas e organizacionais para garantir a segurança do Tratamento.

Ao avaliar o nível adequado de segurança, devem ser considerados os riscos apresentados pelo Tratamento, particularmente em caso de conduta ilegal ou acidental que leve a destruição, perda, alteração, divulgação não autorizada, de ou ao acesso do Dado Pessoal transmitido, armazenado ou de outra forma Tratado.

A adesão a um código de conduta aprovado pela Autoridade Nacional ou um mecanismo de certificação aprovado em linha com e a Lei Geral de Proteção de Dados podem ser utilizados como um elemento para demonstrar a conformidade com a Lei Geral de Proteção de Dados.

O Controlador e o Operador devem garantir que qualquer pessoa que atue sob sua autoridade com acesso aos Dados Pessoais apenas os trate em conformidade com as instruções do Controlador, a menos que exigido de forma diversa pela lei.

INCIDENTE DE SEGURANÇA DE DADOS

A implementação de medidas de segurança no âmbito do o Art. 46 da Lei Geral de Proteção de Dados, juntamente com as medidas previstas na presente Política, devem ser instrumentos apropriados para prevenir incidentes de Segurança de Dados. Na hipótese de um Incidente Segurança de Dados, a gestão deste evento é realizada em cinco etapas que serão reguladas mais detalhadamente por Política específica.

- Detecção: por meio de mecanismos para detecção de Incidentes de Segurança de Dados e emissão de relatório de incidente de segurança;

- Avaliação: Toda advertência que não seja manifestamente infundada deve ser avaliada por um comitê especial para a gestão de incidentes (doravante, o "Comitê de Incidentes"), um grupo coordenado pelo DPO com a tarefa de verificar a existência de um Incidente de Segurança de Dados, identificar os riscos relativos para os direitos e liberdades dos Titulares Pessoais e as consequentes ações a serem implementadas para protegê-los;

- Comunicação: A qualificação de um evento como uma violação de dados gera um processo interno e externo estruturado para cumprir a obrigação de notificar à Autoridade Nacional e ao Titular, dentro um prazo razoável, a depender do caso concreto; em nenhuma hipótese superior a 72 horas e, em nenhum caso, com atraso injustificado. A comunicação deverá ocorrer sempre que houver risco ou dano relevante aos Titulares Pessoais;

- Monitoramento: o monitoramento das atividades deve ser implementado através de infraestruturas dedicadas e salas de controle da situação, a começar pela qualificação do evento como Incidente de Dados e terminando quando concluída a resolução do incidente;

- O registro de violação de dados: qualquer incidente de dados, ainda que não esteja sujeita à notificação à Autoridade Nacional, deve ser adequadamente documentado, incluindo suas consequências e as soluções, dentro de um registro gerenciado pelo Controlador.

PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

- Autenticidade: garantia de que a informação é procedente e fidedigna, sendo capaz de gerar evidências não repudiáveis da identificação de quem a criou, editou ou emitiu.

- Confidencialidade: garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e que sejam devidamente protegidas do conhecimento alheio.

- Disponibilidade: garantia de que as informações e os Recursos de Tecnologia da Informação e Comunicação estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso.

- Integridade: garantia de que as informações estejam fidedignas em relação à última alteração desejada durante o seu ciclo de vida.

GLOSSÁRIO

AGENTES DE TRATAMENTO

Pessoa natural, indicada pelo controlador, que atuará, dessa forma, como um canal entre agentes (controlador e operador), titulares e os órgãos competentes (autoridade nacional).

ANONIMIZAÇÃO

Processos e técnicas por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

É uma entidade que vai ajudar a regular e fiscalizar o cumprimento da Lei Geral de Proteção de Dados. Órgão responsável por caracterizá-lo como uma autoridade pública integrante da Presidência da República. Dentre os atributos estão editar as normas de proteção de dados, monitorar o cumprimento da lei, implementar ferramentas que melhorem a comunicação entre empresas, autoridades e titulares, fazer estudos sobre proteção de dados no exterior e aplicar sanções.

AVISO DE PRIVACIDADE

Em linhas gerais, descreve os tipos de dados pessoais que as empresas coletam, as finalidades para as quais coletam os dados pessoais, os terceiros com as quais as empresas irão compartilhar os dados, as regras para o tratamento dos dados pessoais e as medidas que adotamos para proteger a segurança dos dados.

BANCO DE DADOS

É o conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

BLOQUEIO

Suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

GLOSSÁRIO

CONSENTIMENTO

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

CONTROLADOR

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

DADO PESSOAL

Toda e qualquer informação relacionada a pessoa natural identificada ou identificável. Entre os exemplos de dados pessoais podemos citar o nome, RG, CPF, e-mail, telefone fixo e celular, endereço residencial, etc.

DADO PESSOAL DE CRIANÇA E DE ADOLESCENTE

O Estatuto da Criança e do Adolescente (ECA) considera criança a pessoa até 12 anos de idade incompletos e adolescente aquela entre 12 e 18 anos de idade. Em especial, a LGPD determina que as informações sobre o tratamento de dados pessoais de crianças e de adolescentes deverão ser fornecidas de maneira simples, clara e acessível de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

DADO PESSOAL SENSÍVEL

Todo dado pessoal que pode gerar qualquer tipo de discriminação, tais como os dados 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.

GLOSSÁRIO

DADO PÚBLICO

São as informações publicadas no ambiente digital e facilmente acessadas em modo público, como as redes sociais.

ELIMINAÇÃO

Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

ENCARREGADO (DATA PROTECTION OFFICER – DPO)

É o indicado pelo controlador, denominado Data Protection Officer (DPO) na GDPR, que faz a comunicação entre os titulares que terão seus dados processados e o controlador.

GARANTIA DA SEGURANÇA DA INFORMAÇÃO

Capacidade de sistemas e organizações assegurarem a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação. A Política Nacional de Segurança da Informação (PNSI) dispõe sobre a governança da segurança da informação aos órgãos e às entidades da administração pública federal em seu âmbito de atuação.

INCIDENTE DE SEGURANÇA

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade.

GLOSSÁRIO

LEGÍTIMO INTERESSE

O legitimo interesse é uma das hipóteses legais que autorizam a coleta, armazenamento, mineração ou a transferência de dados pessoais. A rigor, deve ser utilizado de maneira subsidiaria às demais bases legais específicas e surge para atender interesses não do titular, mas do controlador ou de terceiro.

MEDIDAS DE SEGURANÇA

Medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, de acordo como o Art. 46 da Lei Geral de Proteção de Dados e sua respectiva regulamentação.

OPERADOR

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

ÓRGÃO DE PESQUISA

Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

PERFILAMENTO (PROFILING)

A caracterização de perfil refere-se aos métodos e técnicas computacionais aplicados aos dados pessoais ou não dos usuários visando o estabelecimento de um perfil, ou seja, há a utilização legal dos dados para avaliar determinados aspectos pessoais de uma pessoa física, nomeadamente para analisar ou prever aspectos relacionados com o seu desempenho profissional, a sua situação econômica, saúde, preferências pessoais, interesses, confiabilidade, comportamento, localização ou deslocamentos para ofertar produtos, serviços e estabelecer um padrão de consumo, dentre outros.

GLOSSÁRIO

PSEUDONOMIZAÇÃO

Processos e técnicas por meio dos quais um dado tem sua possibilidade de associação dificultada. O dado pseudoanonimizado é considerado dado pessoal para fins de aplicação da Lei Geral de Proteção de Dados, tendo em vista a possibilidade de associação desse dado a uma pessoa natural.

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (DPIA)

É a documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais (Ciclo dos Dados) que podem gerar riscos (Risk Assessment) às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco, tais como mapeamentos, treinamentos, auditorias, alterações de contrato e criação de políticas de proteção de dados.

TERCEIROS

Fornecedores, parceiros e contratados.

TITULAR

Pessoa natural a quem se referem os dados pessoais.

TRANSFERÊNCIA INTERNACIONAL DE DADOS

Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

TRATAMENTO DE DADOS PESSOAIS

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.

GLOSSÁRIO

USO COMPARTILHADO DE DADOS

Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.