CONSELHO DE ARQUITETURA E URBANISMO DE SÃO PAULO – CAU/SP

POLÍTICA INTERNA LEI GERAL DE PROTEÇÃO DE DADOS

Resumo

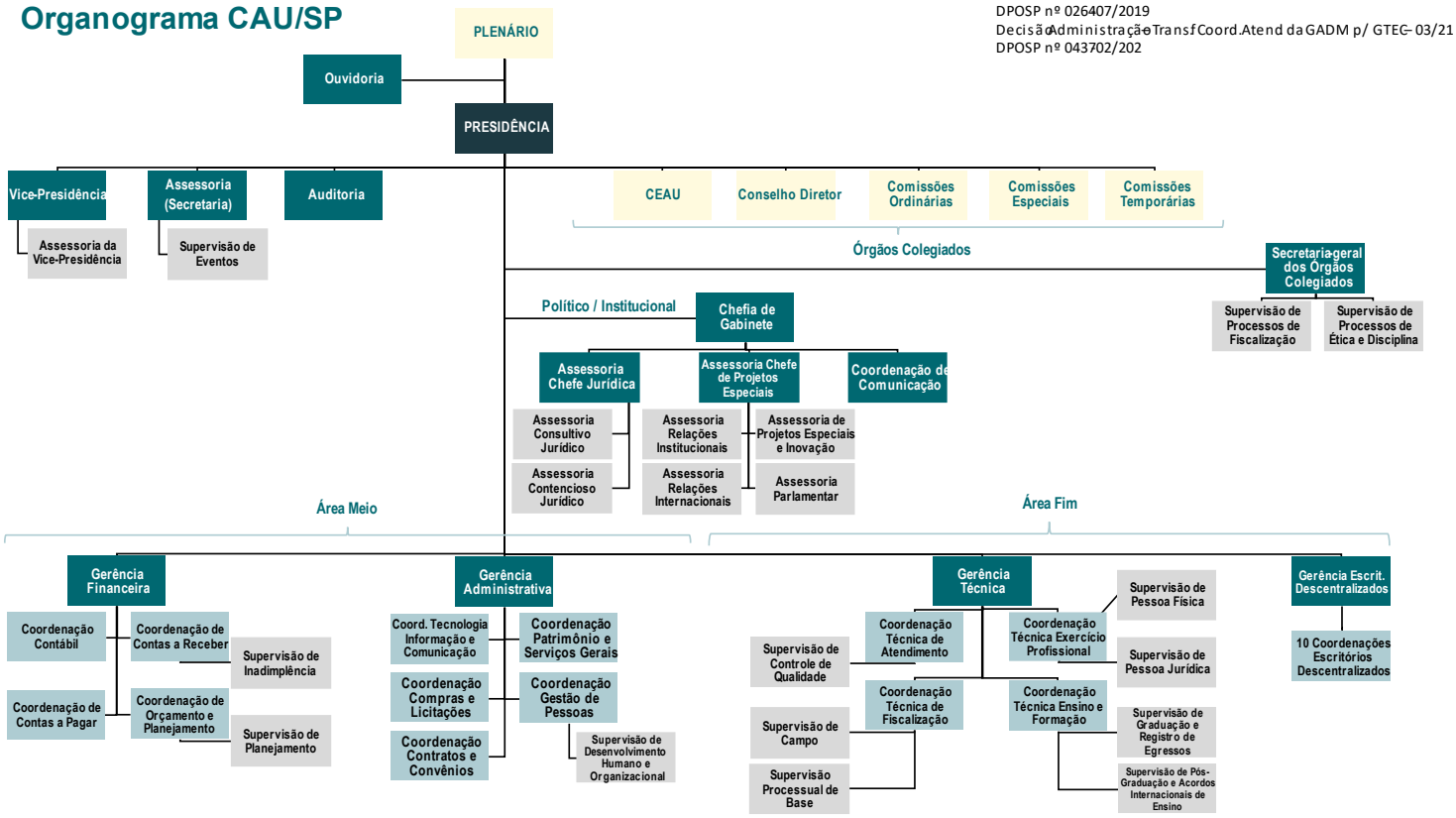
Este documento trata da política interna do Conselho de Arquitetura e Urbanismo de São Paulo – SP visando estabelecer as diretrizes para que as áreas estejam em consonância com a lei geral de proteção de dados

ALBERTO BESSA CONSULTORIA E SERVIÇOS LTDA

Dra. Mara Venditti

1. Política Interna de Proteção de Dados Pessoais

A presente política faz parte do processo de implementação do Conselho de Arquitetura e Urbanismo de São Paulo – CAU/SP para atendimento a lei geral de proteção de dados. Esta política é parte integrante das áreas do CAU/SP.



2. Objetivo

O objetivo desta política é estabelecer diretrizes e regras para o tratamento de dados pessoais realizados pelo **CONSELHO DE ARQUITETURA E URBANISMO DE SÃO PAULO** – **CAU/SP** em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD)

3. Abrangência

Esta política é aplicável a todos os funcionários, servidores e demais pessoas que de alguma forma realizam tratamento de dados pessoais em nome do **Conselho de Arquitetura e Urbanismo de São Paulo – CAU/SP**

4. Princípios do tratamento de dados pessoais e normas internas

O Conselho de Arquitetura e Urbanismo de São Paulo-CAU/SP, pelo presente instrumento vem estabelecer a política de proteção de dados. Considerando a necessidade de implementação de uma política, nos termos da LGPD, e de todos os procedimentos que impliquem o tratamento de dados pessoais, nos serviços, contratos e obrigações, bem como na implantação de sistemas e plataformas que permitam o acesso por parte dos colaboradores ou de terceiros e dados pessoais e/ou tratamento dos dados, os procedimentos aqui descritos servirão como guias para a atuação dos funcionários em conformidade com a LGPD. Nesse sentido, deverão ser observados os seguintes princípios:

Finalidade= Os dados pessoais devem atender a uma finalidade específica, um proposito que seja legitimo, explicito, não sendo permitido tratamento incompatível com as finalidades identificadas.

Adequação= O tratamento de dados pessoais observará a sua compatibilidade com as finalidades de acordo com o contexto do tratamento.

Necessidade= O tratamento dos dados pessoais deve se limitar ao mínimo necessário para a realização das suas finalidades e não deverão conter excessos em relação às finalidades do tratamento.

Qualidade dos dados = Os dados pessoais devem ser claros, exatos, relevantes e atualizados de acordo com a sua necessidade e com os propósitos do tratamento. Não devem ser tratados dados desatualizados.

Transparência= O Conselho de Arquitetura e Urbanismo de São Paulo- CAU/SP deve dispor de informações claras, precisas e acessíveis desde que obedeça a base legal implementada a cada tratamento.

Segurança= Todas as informações que contenham dados pessoais devem ser mantidas em segurança técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ilícitas de destruição, perda, alteração, comunicação ou difusão.

Prevenção= O Conselho de Arquitetura e Urbanismo de São Paulo- CAU/SP adotara medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Não discriminação= O Conselho de Arquitetura e Urbanismo de São Paulo - CAU/SP jamais realizará tratamento para fins discriminatórios ilícitos ou abusivos.

Responsabilização e Prestação de Contas= O Conselho de Arquitetura e Urbanismo de São Paulo- CAU/SP adotará medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de dados pessoais, e inclusive, a eficácia dessas medidas.

5. Tratamento de dados pessoais

A Lei Geral de Proteção de Dados (LGPD) permite o tratamento de dados pessoais apenas para fins específicos e legítimos, como a prestação de serviços públicos. O tratamento deve ser transparente e seguro, e a lei estabelece regras claras e objetivas para garantir que seja realizado com ética e responsabilidade.

Nesse sentido, destaca-se que a política geral do Conselho de Arquitetura e Urbanismo de São Paulo – CAU/SP em atenção à Lei Geral de Proteção de Dados respeitará o ciclo de dados pessoais para que o tratamento dos dados seja realizado com eficiência e comprometimento.

6. Boas práticas na aplicação da política de dados:

- ✓ Proteção dos dados contra acesso não autorizado, uso indevido e divulgação
- ✓ Usar os dados para os fins coletados
- ✓ Acesso a correção e exclusão dos dados quando necessários, observados dos princípios e bases legais estipuladas para a administração pública.

7. Ciclo de dados Pessoais

A presente política obedecerá ao ciclo de dados pessoais decorrentes do tratamento da lei geral de proteção de dados. O ciclo deverá possuir:

- ✓ **Coleta**
- ✓ **Armazenamento**
- ✓ **Compartilhamento**
- ✓ **Descarte**

Os procedimentos inerentes a coleta de dados pessoais serão procedidos para cada área, sendo que deverão ser observados a essência da coleta sem

excessos, ou seja, cada área determinará como coletará seus dados para atender as demandas diárias.

As coletas poderão ser realizadas por:

- ✓ Sistemas
- ✓ e-mails institucionais
- ✓ formulários padronizados (se necessário)
- ✓ planilhas padronizadas (se necessário)
- ✓ documentos físicos (se necessário, evitar este procedimento)
- ✓ ou outros documentos estipulados pela administração pública desde que atendam às exigências da lei geral de proteção de dados.

Os dados coletados poderão ser diferenciados pelas áreas e poderão ser coletados através de:

- ✓ Dados pessoais coletados de clientes;
- ✓ Dados pessoais coletados de funcionários;
- ✓ Dados pessoais coletados de fornecedores;
- ✓ Dados pessoais de visitantes presenciais
- ✓ Dados pessoais coletados através do site;
- ✓ Dados pessoais de representantes;
- ✓ Dados pessoais de terceiros;
- ✓ Dados pessoais de profissionais técnicos;

Os dados coletados devem ter uma finalidade específica para o tratamento. Para isso, é importante evitar coletar dados desnecessários ou excessivos.

Todos os dados pessoais devem ser categorizados pelas áreas.
Sendo definidos como:

- ✓ Dados pessoais comuns;
- ✓ Dados pessoais sensíveis;
- ✓ Dados de crianças e adolescentes (quando for o caso);

Os procedimentos de coleta deverão ser observados por todas as áreas da Administração Pública e devem fazer parte dos procedimentos das rotinas diárias.

Armazenamento

Após a coleta, os dados devem ser armazenados e devem permanecer em local seguro. Os locais onde são armazenados os dados pessoais devem possuir proteção contra acessos não autorizados.

Os locais de armazenamento dos dados também deverão garantir o mapeamento de qualquer alteração realizada, bem como possuir ferramentas que evitem a perda, destruição, alterações indevidas dentre outras atividades prejudiciais à mantença da integridade, segurança, confiabilidade e autenticidade dos documentos arquivados/armazenados em sistemas digitais ou meios físicos.

Os locais de armazenamento devem conter senhas fortes e criptografia. As senhas devem ser fortes, e sugere-se a troca periodicamente, sob supervisão da área de tecnologia da informação.
Todos os procedimentos de criação e troca de senhas serão orientados pela área de Tecnologia da Informação".

Se necessário os dados poderão ser criptografados para segurança do armazenamento.

O controle de acesso deve ser restrito a funcionários autorizados. Somente pessoas autorizadas poderão ter acesso aos dados armazenados

E, ainda no tocante ao armazenamento é de suma importância destacar os procedimentos de backup, ou seja, armazenados com backup seguro para evitar a perda de dados em caso de incidente.

Para garantir a segurança do armazenamento, recomenda-se a realização de auditorias internas periódicas.

Devem ser adotadas medidas técnicas e administrativas para garantir a segurança do armazenamento. As medidas devem ser adequadas a natureza dos dados pessoais e aos riscos envolvidos.

Compartilhamento

O compartilhamento de dados deve ser analisado para que esteja em acordo com a Lei Geral de Proteção de Dados e ainda, observar todos os critérios e as finalidades essenciais para que ocorra o compartilhamento.

E, ainda se faz necessário a observância das categorias de compartilhamento, sendo eles:

Compartilhamento interno= dados compartilhados entre as áreas
Compartilhamento de dados pessoais compartilhados entre todas as áreas do Conselho de Arquitetura e Urbanismo de São Paulo- CAU/SP

Compartilhamento externo= dados compartilhados com terceiros, como fornecedores, parceiros, prestadores de serviços, profissionais técnicos, órgãos públicos, agências reguladoras, bancos, instituições financeiras, empresas privadas, agências de marketing, entre outros que estejam ligados aos procedimentos inerentes ao Conselho de Arquitetura e Urbanismo de São Paulo- CAU/SP

Compartilhamento internacional= Decorre de situações que envolvam transferência de dados internacionais (somente se for o caso)

Os dados compartilhados devem possuir segurança no que concerne o seu compartilhamento, observando as finalidades.

Todas as áreas devem se atentar ao uso do compartilhamento dos dados, observando que estes devem ser compartilhados com as pessoas através de suas finalidades para o atendimento as demandas.

A presente política aplica-se a todos os membros do organograma do Conselho de Arquitetura e Urbanismo de São Paulo- CAU/SP.

Todas as áreas do Conselho de Arquitetura e Urbanismo de São Paulo- CAU/SP devem obedecer às diretrizes de compartilhamento da lei geral de proteção de dados. Todas as áreas deverão reestruturar suas rotinas para atendimento a Lei Geral de Proteção de Dados e ainda, proceder com o ciclo de dados pessoais corretamente.

Descarte

Os procedimentos de descarte fazem parte da política de proteção de dados e devem ser seguidos adequadamente. Todas as áreas deverão observar os métodos de descarte de dados. Para ocorrer o descarte, se faz necessário seguir a tabela de temporalidade.

A tabela de temporalidade decorre de instrumento de gestão documental que determinará o prazo de retenção e destinação. Esse procedimento encontra-se elencado para atendimento a Lei Geral de Proteção de Dados para que se proceda com o descarte que faz parte do ciclo de dados pessoais.

A tabela de temporalidade deve sempre se atentar a legislação vigente.
A tabela de temporalidade do Conselho de Arquitetura e Urbanismo de São Paulo - CAU/SP obedece a tabela do Arquivo Nacional e demais correlatas se necessário.

O período de retenção se refere ao armazenamento e posterior descarte após atingir a finalidade e observância da tabela de temporalidade.

Destacamos as situações que devem ser observadas e fazem parte da presente política:

Preservação= documento mantido no arquivo
Transferência = Poderá ser transferido para arquivo terceirizado
Destruição = os documentos devem ser destruídos de forma segura, se atentando às orientações das autoridades responsáveis e à tabela de temporalidade do Arquivo Nacional.

Os dados pessoais descartados devem ser identificados e separados dos demais dados.
Os procedimentos de descarte devem ser específicos sobre os métodos de que serão utilizados.

Destruição física = trituração, incineração e fragmentação.
Destruição lógica= decorre de descarte de dados pessoais que remove os dados de dispositivo que se encontram armazenados.
Para processos físicos sugere-se fragmentadora de papéis
Para mídias sugere-se fragmentadora de mídias (se for o caso)

O setor de tecnologia da informação deverá se atentar aos procedimentos de descarte de que tratam os processos lógicos que não decorrem de documentos físicos.

O processo de anonimização faz parte integrante da política de dados e deve ser observados os métodos inerentes para que se conclua o descarte dessa maneira.
Este método torna os dados pessoais não identificáveis
Os métodos de anonimização incluem:

I. Remoção de dados pessoais, ou seja, os dados pessoais são removidos dos dados.
II. Agremiação dos dados pessoais, estes são agrupados de forma que não seja possível identificar os titulares de dados

Equipamentos que poderão ser utilizados nos processos de descarte:

- ✓ Fragmentadora de papeis, incineradores e dispositivo de fragmentação de dados
- ✓ Softwares de sobrescrita de dados e dispositivos de desmagnetização
- ✓ Anonimização são utilizados softwares de anonimização de dados

Modelos de software de anonimização de dados que poderão ser utilizados pelo Conselho de Arquitetura e Urbanismo de São Paulo-CAU/SP.

- ✓ ARX
- ✓ Data Shield
- ✓ Pseudonymizer
- ✓ Redcap

Os softwares de anonimização de dados serão avaliados pela área de tecnologia da informação do Conselho de Arquitetura e Urbanismo de São Paulo – CAU/SP das quais atenderão com eficácia a demanda, se houver a necessidade de procederem com o descarte através de anonimização.

É dever de todos conhecer a política e entender os processos de descarte que serão desenvolvidos nas rotinas.

O descarte deve ser procedido adequadamente, não poderão ocorrer descartes inadequados aos métodos empregados.

É importante observar os locais que serão procedidos os descartes dos dados pessoais.

Todos os dados pessoais decorrentes obedecerão aos métodos e processos decorrentes desta política. Como elucidado, cada área possui sua rotina diária

e independentemente se as rotinas sofrem mudanças, é primordial que todas sigam as orientações decorrentes da política de dados.

8. Documentos/E-mails/ Sistemas / Procedimentos internos

1. Todos os documentos serão revisados sempre que necessário adotando métodos de acordo com a lei geral de proteção de dados.

2. Contratos que envolvam todas as áreas deverão ser revisados com a inserção de cláusulas contratuais de acordo com a LGPD.

3. Contratos e aditivos que decorram de demandas licitatórias devem conter expressamente cláusulas de acordo com a lei geral de proteção de dados.

4. Formulários e planilhas serão revisados e não constarão dados em excesso, somente o que for necessário para atendimento as finalidades do caso concreto.

5. Demais documentos que venham a ser criados serão observados todos os critérios de acordo com a lei geral de proteção de dados.

6. Todos os e-mails (institucionais) encaminhados devem conter no corpo do e-mail informações acerca da Lei Geral de Proteção de Dados, visando que o receptor tenha ciência de que o Conselho de Arquitetura e Urbanismo de São Paulo - CAU/SP se encontra de acordo com a lei.

7. Após o recebimento de documentos por e-mail, se estes forem inseridos em sistemas, os e-mails devem ser descartados, conforme tabela de temporalidade. Caso não exista prazo definido na tabela, deve ser estabelecido um prazo específico para cada setor ou área. Isso porque, se os documentos e as informações já estão nos sistemas, não há necessidade de manter os e-mails. A Lei Geral de Proteção de Dados (LGPD) proíbe o excesso no tratamento de dados pessoais.

8. Mensagem que deverá conter no corpo do e-mail: **Todos os e-mails encaminhados pelo Conselho de Arquitetura e Urbanismo de São Paulo – CAU/SP encontram-se de acordo com a Lei Geral de Proteção de Dados.**

9. Todos os contratos que decorram de licitações deverão ser assinados pelas partes através do SEI. O licitante deverá possuir cadastro para que os atos sejam oficializados através do sistema, visando assegurar proteção das informações.

10. Solicitação de dados pessoais não poderão ser realizadas aleatoriamente ou verbalmente, todos os atos que envolvam a solicitação de dados pessoais devem possuir documentos oficiais do Conselho de Arquitetura e Urbanismo de São Paulo – CAU/SP, sejam através de ofícios, formulários entre outros. É de suma importância que a Lei Geral de Proteção de Dados seja respeitada.

O encarregado de dados e comitê gestor farão análises dos documentos que decorrerão de mudanças, bem como o departamento juridico do Conselho de Arquitetura e Urbanismo de São Paulo – CAU/SP.

11. Crachás

A área responsável deve, sempre que for necessário modificar dados, observar os requisitos estabelecidos pela Lei Geral de Proteção de Dados (LGPD) e pelas necessidades do Conselho de Arquitetura e Urbanismo de São Paulo CAU/SP.

12. Termos de Confidencialidade e Imagem

1. O termo de confidencialidade é um documento obrigatório nos procedimentos internos do Conselho de Arquitetura e Urbanismo de São Paulo - CAU/SP. Ele deve ser assinado por todos os envolvidos,

incluindo fornecedores, terceiros, funcionários e outros, que tenham acesso a informações confidenciais do Conselho de Arquitetura e Urbanismo de São Paulo - CAU/SP.

2. O termo deve definir quais serão as informações confidenciais, podendo ser dados pessoais, informações técnicas, administrativas, comerciais ou quaisquer informações que sejam consideradas sigilosas para o Conselho de Arquitetura e Urbanismo de São Paulo - CAU/SP.

3. O termo deve definir o período de sua vigência a ser utilizado

4. O termo deve ainda estabelecer as obrigações de confidencialidade das partes envolvidas, por exemplo: não divulgar, utilizar ou compartilhar as informações confidenciais.

5. O termo deverá ser utilizado por todas as áreas do CAU/SP sempre que houver a necessidade.

6. O modelo do termo de confidencialidade será único para todas as áreas

7. O termo deve prever sanções para o seu descumprimento como multas, indenização ou rescisão contratual.

13. Termo de uso de imagem

1. O Conselho de Arquitetura e Urbanismo de São Paulo - CAU/SP adotará termo de uso de imagem sempre que for necessário, visando a obediência a lei geral de proteção de dados.

2. A imagem é um dado pessoal e deve ser tratado de acordo com a LGPD.

3. O termo deverá ser claro, objetivo e em linguagem acessível, visando atender a finalidade do uso da imagem.

4. O termo deve especificar claramente as finalidades para qual a imagem será utilizada.

5. O termo poderá estabelecer período da autorização e quanto tempo permanecerá válida

6. O termo se fará necessário sempre que o Conselho de Arquitetura e Urbanismo de São Paulo – CAU/SP verificar a necessidade do uso da imagem a qual deva atender a lei geral de proteção de dados.

7. A imagem não pode ser utilizada para fins discriminatórios ou difamatórios etc.

14. Funcionários, Servidores, Estagiários, Colaboradores, Fornecedores, Terceiros entre outros.

1. Todos devem ter ciência da Lei Geral de Proteção de Dados incluindo seus princípios e diretrizes.

2. Todos devem tomar as medidas necessárias para a proteção dos dados pessoais, evitando acessos não autorizados, vazamentos ou outros incidentes de segurança.

3. A violação das responsabilidades pode resultar em sanções administrativas como multas, responsabilidade civil e criminal.

4. Deve se atentar aos procedimentos que envolvam o tratamento dos dados de acordo com ciclo de dados pessoais e as bases legais.

5. Os procedimentos acima também se aplicam a fornecedores, terceirizados, profissionais técnicos entre outros.

15. Entrada de visitantes /Recepção

As informações solicitadas aos visitantes devem ser as mínimas possíveis, ou seja, as essenciais para identificar a pessoa.

- ✓ Nome, CPF e a qual setor pretende se dirigir, com quem pretende conversar/obter informações/ reunir/ obter documentos etc. (dados do interlocutor).

As informações devem ser registradas em sistema próprio ou, no mínimo, em planilha de Excel. Elas devem ser armazenadas em local seguro, preferencialmente na nuvem. Após a conclusão de sua finalidade, devem ser descartadas, conforme previsto na tabela de temporalidade.

Empresas terceirizadas são responsáveis também pelo manuseio destas informações.

Após a conclusão das obras na sede do Conselho de Arquitetura e Urbanismo de São Paulo - CAU/SP, quando do ingresso no prédio deverão ser fornecidos crachás aos visitantes.

16. Arquivos físicos

Local seguro – O arquivo fisico deve permanecer em local seguro, protegido de acesso não autorizado, roubo ou perda. O local poderá ser salas que permaneçam trancadas, ou ainda contar com um profissional arquivista que cuide do acervo e quaisquer documentos que sejam retirados do local deverá conter a informação de entrada e saída.

Acesso restrito- O acesso ao arquivo deve ser restrito a pessoas autorizadas. Para isso, deve ser implementado um sistema de controle de acesso, que pode ser de diversas formas, como senhas, biometria ou outros meios que o Conselho de Arquitetura e Urbanismo de São Paulo – CAU/SP determinar.

Organização adequada- A organização dos documentos deve facilitar o acesso e a localização das informações. Isso pode ser feito por meio de um sistema de inventário ou de classificação, ou ainda por empresas terceirizadas.

Proteção contra danos – Os documentos devem ser protegidos contra danos físicos, como fogo, água, deterioração, deve ser armazenado em local adequado e climatizado.

Destruição segura - Os documentos que cumpriram a sua finalidade, atingiram o tempo decorrente da tabela de temporalidade, deverão ser descartados de maneira segura, de modo a impedir a recuperação das informações, podendo ser feito por trituração, incineração, ou outros métodos de destruição.

17. Manual de normas e procedimentos das áreas

Todas as áreas deverão ter seu manual de normas e procedimentos e este deve ser auditado e ainda deverão estar de acordo com as legislações pertinentes, incluindo a lei geral de proteção de dados.

I. Os manuais deverão ser claros e concisos.
II. Devem ser atualizados regularmente.
III. Devem ser divulgados aos funcionários para que eles estejam cientes das normas e procedimentos adotados.
IV. Deverão definir as responsabilidades de cada área.
V. E no tocante a Lei Geral de Proteção de Dados deverão obedecer aos procedimentos elencados na política interna.

Os manuais de normas e procedimentos do Conselho de Arquitetura e Urbanismo de São Paulo – CAU/SP encontram-se em elaboração e em análise pela auditoria.

Deve ser estabelecido prazo para a implantação do manual de normas e procedimentos das áreas.

Comitê gestor deverá acompanhar os procedimentos com a área de auditoria.

18. Uso de WhatsApp

Preferencialmente não se deve enviar documentos que contenham dados pessoais via WhatsApp.

As áreas de atendimento que utilizam o WhatsApp como ferramenta de acesso aos usuários devem contar com uma conta comercial do WhatsApp e um link com opções de atendimento para os usuários. Essas opções devem ser claras e objetivas, de modo a permitir que os usuários escolham o canal de atendimento que mais lhes convém.

Deve ser informado que o uso do WhatsApp quando se tratar de atendimento está de acordo com a Lei Geral de Proteção de Dados.

O WhatsApp permite que os usuários configurem as mensagens para que sejam excluídas automaticamente após um determinado período. Essa função é útil para proteger a privacidade dos usuários, de acordo com a Lei Geral de Proteção de Dados (LGPD).

Os dados coletados devem ser apenas o necessário para fornecer o atendimento ao cliente, deve ser informado ao usuário que os dados fornecidos são usados para o atendimento solicitado e encontram -se sobre a proteção da Lei Geral de Proteção de Dados (informações automáticas).

19. WhatsApp interno

O uso do WhatsApp para fins internos deve ser restrito à comunicação essencial entre funcionários, clientes e fornecedores. As informações devem ser relevantes para o trabalho e devem evitar o trânsito de anexos de documentos pessoais. Quando isso for necessário, os anexos devem ser descartados por meio de mensagens temporárias.

As comunicações internas pelo WhatsApp decorrem do meio de comunicação eficaz, é de suma importância que todos tenham atenção ao seu manuseio e a responsabilidade das informações decorrentes. Sempre visando o atendimento a Lei Geral de Proteção de Dados.

20. As hipóteses de tratamento de dados pessoais – Base Legal

O Conselho de Arquitetura e Urbanismo de São Paulo- CAU/SP somente tratará dados pessoais de acordo com as hipóteses autorizadas pela LGPD.

- ✓ **Cumprimento de obrigação legal ou regulatória; art.7, II, LGPD**

A LGPD permite que o tratamento de dados pelo Poder Público seja realizado para o cumprimento de obrigação legal ou regulatória, conforme art. 7º, II e art. 11, II, a. O conceito de obrigação legal é reforçado no art. 23, quando destaca que o tratamento de dados pessoais no setor público deverá ser realizado com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público", observando, ainda, o interesse público e o atendimento da finalidade pública do controlador. (https://www.migalhas.com.br/depeso/360877/lgpd-no-setor-publico-bases-legais-para-o-tratamento-de-dados)

1. Tratamento pela administração pública, art.7, III, LGPD
2. Execução ou preparação contratual, art.7, V, LGPD
3. Exercício regular de direitos em processo judicial, administrativo ou arbitral; art.7, VI, LGPD

19. Segurança da informação

O Conselho de Arquitetura e Urbanismo de São Paulo – CAU/SP adotará medidas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados, destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

20. Incidentes de segurança

Em caso de incidente de segurança que possa acarretar risco ou dano relevante aos titulares de dados pessoais, o CAU/SP Conselho de Arquitetura e Urbanismo de São Paulo adotará as seguintes medidas:

- Identificação do incidente: Identificar o incidente e avaliar o seu impacto nos titulares de dados pessoais.
- Comunicação aos titulares: Comunicar o incidente aos titulares de dados pessoais afetados, de forma clara e concisa, em prazo razoável.
- Investigação e remediação: Investigar o incidente e adotar as medidas necessárias para remediar os danos causados.

21. Registro de atividades de tratamento

O Conselho de Arquitetura e Urbanismo de São Paulo- CAU/SP manterá um registro das atividades de tratamento de dados pessoais, contendo as seguintes informações:

- **Finalidade do tratamento;
- **Descrição das atividades de tratamento;
- **Categorias de dados pessoais tratados;
- **Destinatários dos dados pessoais;
- **Período de retenção dos dados pessoais;
- **Medidas de segurança adotadas;
- **Eventuais transferências internacionais de dados;
- **Eventuais incidentes de segurança.

Esta Política de Dados deve ser conhecida por todos do Conselho de Arquitetura e Urbanismo de São Paulo - CAU/SP. Ela estabelece as diretrizes da Lei Geral de Proteção de Dados (LGPD) para as rotinas diárias de todas as áreas do Conselho de Arquitetura e Urbanismo de São Paulo - CAU/SP.

Demais situações não previstas e não elencadas serão analisadas pelo encarregado de dados e comitê gestor visando estabelecer as regras a serem adotadas em cada caso concreto.

Todos os procedimentos serão analisados e adotados a fim de resolução imediata para estabelecer a ordem interna e externa dos dados pessoais.

O Conselho de Arquitetura e Urbanismo de São Paulo - CAU/SP obedecerá às normas de acordo com a legislação e todos os métodos externos serão analisados sob a ótica da regularidade perante a ANPD e lei geral de proteção de dados.

22. Atualização

Esta política poderá ser atualizada a qualquer momento, a critério do Conselho de Arquitetura e Urbanismo de São Paulo - CAU/SP – Conselho de Arquitetura e Urbanismo de São Paulo

23. Disposições finais

Esta política é parte integrante do Conselho de Arquitetura e Urbanismo de São Paulo - CAU/SP.

São Paulo, 01 de novembro de 2023.

Encarregado de dados (DPO as a Service)
Dra. Mara Cristhiane Venditti Borges
OAB nº 437967

Comitê Gestor:

Ana Claudia Galeazzo
Amanda Cristina Silvério
Daiane Fernandes do Vale
Eduardo da Silva Pinto
Gabriela Martins Raimundo
Mariana Fialho Nascimento
Thiago Pereira Machado
Rodrigo Delfino Carvalho
Ronaldo Rodrigues