ABEP

Associação Brasileira de Empresas de Pesquisa

POLÍTICA CORPORATIVA
PROTEÇÃO DE DADOS PESSOAIS
ABEP

Abril de 2021

ESCOPO

Esta política visa estabelecer as diretrizes e princípios para a devida coleta, tratamento e armazenamento de dado pessoal pela ABEP, aplicando-se a todas as informações pessoais tratadas tanto no meio físico quanto no meio eletrônico.

Esta política também envolve todos os colaboradores, filiados, parceiros, fornecedores e prestadores de serviço que, de alguma forma, tratem ou tenham acesso aos dados pessoais controlados/operados pela ABEP.

Ressalte-se que além das regras e princípios desta Política, será necessário que todo tratamento de dados seja realizado cuidadosamente nos limites das leis vigentes no Brasil e de parâmetros éticos e sociais. É de expectativa da ABEP que os filiados, parceiros e colaboradores adotem esses cuidados mínimos; caso contrário, será impossível a manutenção de uma relação de confiança, o que consequentemente, impossibilita a manutenção de relações empresariais duradouras.

Desta forma, nenhum colaborador, parceiro ou filiado está autorizado a estipular regulamentações divergentes desta Política, e no caso de sua existência, as orientações da presente Política prevalecerão sobre as demais.

Eventuais alterações nesta Política serão analisadas e aprovadas pelo Comitê de Proteção de Dados Pessoais da ABEP e pelo Encarregado de Proteção de Dados Pessoais da ABEP.

Constituem parte integrante desta Política Corporativa de Proteção de Dados Pessoais, sem prejuízo de outras que venham a ser criadas/estabelecidas a Política de Privacidade do sítio eletrônico da ABEP.

No caso de conflito entre qualquer anexo e esta Política Corporativa de Proteção de Dados Pessoais, prevalecerão as regras contidas nesta Política.

Esta política deverá ser distribuída para todo colaborador, filiado, parceiro comercial e/ou prestador de serviços da ABEP, mediante comprovação de recebimento e ciência.

CONTEÚDO

DEFINIÇÕES

Filiado: pessoa, física ou jurídica, associada à ABEP, ou que esteja avaliando a possibilidade de torna-se um filiado da ABEP.

Dado pessoal: toda e qualquer informação que, isolada ou conjuntamente com outras informações fornecidas, permitam a identificação e individualização de quem as forneceu (ex. RG, CPF, nome, endereço, IP).

Dado sensível: dados pessoais sobre a origem racial ou étnica, convicções religiosas, dados referentes à saúde, à vida sexual, além de dados genéticos e biométricos (reconhecimento facial, voz, digital, íris).

Dados anonimizados: dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Tratamento de Dados: 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.

Banco de dados: conjunto estruturado de dados pessoais em formato eletrônico ou físico.

Titular de dados: pessoa natural a quem se referem os dados pessoais objeto de tratamento.

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões sobre tratamento de dados pessoais.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Encarregado de dados: pessoa natural ou jurídica indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados – ANPD.

Base legal para o tratamento de dados pessoais: fundamento legal utilizado a fim de conceder licitude ao tratamento de dados pessoais. A LGPD enumera dez bases, sendo estas: (i) consentimento do titular;

(ii) obrigação legal ou regulatória pelo controlador; (iii) pela administração pública; (iv) para a realização de estudos por órgão de pesquisa; (v) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; (vi) para o exercício regular de direitos em processo judicial, administrativo ou arbitral; (vii) para a proteção da vida ou da incolumidade física do titular ou de terceiro; (viii) para a tutela da saúde; (ix) quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; (x) para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Consentimento: manifestação livre (que permita a escolha do titular), informada (informação presente e acessível) e inequívoca (cujo consentimento não deixa dúvidas) pela qual o titular concorda com o tratamento de seus dados pessoais para a finalidade informada.

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

Violação de dados pessoais: uma violação da segurança, acidental ou ilícita, que consista na destruição, perda, alteração, divulgação ou no acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

PRINCÍPIOS PARA O PROCESSAMENTO DE DADOS PESSOAIS

Toda operação envolvendo dados pessoais deve sempre observar os princípios norteadores para o manuseio e tratamento dos dados. A LGDP – Lei Geral de Proteção de Dados (art. 6º) enumera 10 princípios fundamentais, sendo eles:

FINALIDADE: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

ADEQUAÇÃO: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

NECESSIDADE: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

LIVRE ACESSO: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

QUALIDADE DOS DADOS: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

TRANSPARÊNCIA: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

SEGURANÇA: 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;

PREVENÇÃO: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

NÃO DISCRIMINAÇÃO: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

NÃO APLICAÇÃO

Esta Política Corporativa de Proteção de Dados não se aplica a análises estatísticas ou inspeções efetuadas com base em dados pessoais anonimizados, anônimos ou em qualquer das hipóteses previstas no art. 4º da Lei Geral de Proteção de Dados Pessoais.

POLÍTICAS ESTABELECIDAS

Diretrizes gerais

Os dados pessoais coletados ou recebidos pela ABEP, seja de colaboradores, empregados, filiados, parceiros, fornecedores e prestadores de serviço, devem necessariamente seguir os padrões de coleta, armazenamento, tratamento e descarte instituídos na presente Política.

A coleta de dados pessoais é realizada para legitimar relações administrativas e comerciais, tais como, mas não se limitando as seguintes: administração de segurança e desempenho; informações de contato; recursos humanos; viabilização de negócios e prestação de serviços; desenvolvimento de pesquisas; entre outras finalidades que forem estipuladas pela ABEP.

A ABEP compromete-se a utilizar os dados de forma consistente com esta Política e com a legislação vigente sobre o tema. Todas as informações pessoais coletadas ou recebidas serão utilizadas para fins legítimos.

Na hipótese da ABEP ser classificada como Operadora dos Dados Pessoais, será necessário certificar-se que, apesar de tratar os dados pessoais sob a restrita orientação lícita do Controlador, as informações tratadas estejam em conformidade com a presente Política e com a legislação vigente, com registro de, no mínimo, finalidade, base legal, origem dos dados pessoais tratados e compartilhamento.

Coleta/uso de dados

Sobre a coleta de dados, é necessário que o Controlador de Dados Pessoais forneça ao titular informações exigidas pelas leis e regulamentos aplicáveis e, pelo menos, a identidade e os detalhes de contato do Controlador de Dados e de seu Encarregado de Dados, se houver; com explicação sobre os objetivos do processamento; os destinatários ou categorias de destinatários dos seus dados pessoais; e a existência dos direitos dos titulares de dados pessoais.

A operação de tratamento de dados pessoais deverá se basear em uma destas hipóteses:

- consentimento (escrito ou através de meio que demonstre a vontade do titular);
- obrigação legal;
- pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;

- para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- necessidade para execução contratual;
- exercício regular de um direito;
- proteção à vida ou incolumidade física do titular ou de terceiros;
- para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- para atender a legítimo interesse do controlador ou de terceiros;
- para a proteção de crédito; e,
- em razão da publicidade dada aos dados pelo próprio titular, resguardadas as finalidades e direitos previstos na LGPD.

Caso o tratamento dos dados pessoais não tenha como fundamento uma das bases legais acima descritas, o tratamento dos dados pessoais será considerado ilícito. O agente de tratamento dos dados pessoais deverá, ainda, obedecer aos princípios elencados na LGPD (art. 6º), em especial os princípios da finalidade e da transparência.

Caso o dado pessoal coletado seja classificado como sensível, será necessário o consentimento específico e destacado do titular de dados para o tratamento. Se não houver consentimento, o tratamento só poderá se dar para:

- Cumprimento de obrigação legal ou regulatória pelo controlador;
- Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
- Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
- Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
- Proteção da vida ou da incolumidade física do titular ou de terceiros;
- Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da LGPD e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;

Em todo o tratamento de dados pessoais que houver risco às liberdades civis e aos direitos fundamentais – inclusive legitimo interesse e dados sensíveis – a ABEP entende ser necessária a elaboração do

Relatório de Impacto (DPIA), que deve conter a descrição dos processos de tratamento de dados pessoais, bem como medidas, salvaguardas e mecanismos de mitigação de risco, assim detalhado:

- ❑ descrever a natureza, escopo, contexto e propósitos do processamento;
- ❑ avaliar a necessidade, proporcionalidade e medidas de conformidade;
- ❑ identificar e avaliar os riscos para os indivíduos; e
- ❑ identificar quaisquer medidas adicionais para mitigar esses riscos.

Direitos dos Titulares

A ABEP está comprometida em garantir a proteção de seus direitos sob as leis aplicáveis, incluindo o respeito aos direitos dos titulares de dados pessoais, a ser exercido mediante solicitação destinada ao Encarregado de Dados Pessoais (lgpd@abep.org).

Direito de Confirmação da Existência de Tratamento	O titular possui o direito de receber confirmação sobre a existência de tratamento de seus dados pessoais.
Direito de acesso	O titular pode solicitar acesso aos seus dados pessoais, assim como, a correção de dados pessoais imprecisos ou incompletos, além de poder solicitar uma cópia dos dados pessoais tratados pelo Controlador.
Direito de Retificação	O titular pode solicitar a correção dos dados incompletos, inexatos ou desatualizados.
Direito de Eliminação dos Dados Pessoais	O direito de eliminação concede ao titular o direito de solicitar a exclusão de seus dados pessoais nos casos em que: ✓ os dados não são mais necessários; ✓ houver retirada do seu consentimento; ✓ os dados pessoais foram processados ilegalmente; ✓ existir uma obrigação legal de apagar seus dados pessoais.
Direito de Portabilidade	A portabilidade dos dados pessoais fornecidos, em um formato estruturado, comumente utilizado. O titular possui o direito de transmitir esses dados para outro Controlador ou a terceiro escolhido, sem impedimentos.
Direito de Informação	O titular possui o direito de ser informado, de maneira clara e acessível, sobre: ✓ a coleta e uso de seus dados pessoais, sendo necessário garantir ao titular de dados informações como o propósito do tratamento de dados, o período de retenção, e com quem será compartilhada a informação; ✓ a possibilidade de não fornecer o consentimento e as consequências de sua negativa; ✓ as entidades públicas ou privadas com as quais o Controlador realizou compartilhamento de seus dados pessoais.
Revogação do Consentimento	O titular tem o direito de solicitar a revogação do consentimento, quando o tratamento de dados tiver como fundamento a base legal do consentimento.
Direito de oposição ao processamento para fins de marketing (ou outro processamento fundado no consentimento ou legítimo interesse)	Oposição ao processamento dos dados pessoais, particularmente em relação à criação de perfis ou às comunicações de marketing. Quando há processamento, mediante consentimento, este poderá ser retirado pelo titular de dados pessoais a qualquer momento.
Direito de Solicitar Revisão ao Tratamento Automatizado	Solicitar a revisão de decisão tomada unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

Sobre o atendimento das solicitações dos titulares, faz-se necessário que a resposta com informações aos titulares seja:

- ❑ Concisa
- ❑ Transparente
- ❑ Compreensível
- ❑ Facilmente acessível; e
- ❑ Utilizada linguagem simples e clara.

Faz-se importante que o Controlador de Dados Pessoais informe ao Titular de Dados sobre seus Direitos, bem como garanta os meios para que ele os exerça. Frise-se que nas relações das quais a ABEP é classificada como Operadora de Dados Pessoais, a ABEP não poupará esforços para auxiliar o Controlador com eventual demanda atrelada aos serviços prestados pela ABEP.

As solicitações deverão ser respondidas em até 7 dias úteis, contados da data da solicitação. Na hipótese deste prazo não ser suficiente para a formalização da resposta adequada ou do cumprimento da solicitação, deverá ser enviada uma resposta explicando o ocorrido e informando que a resposta será enviada, impreterivelmente em mais 15 dias úteis.

Na hipótese de a solicitação tratar sobre a confirmação de existência de tratamento de dados pessoais pela ABEP ou sobre o acesso aos dados pessoais em controle da ABEP, a resposta deverá ser dada de maneira simplificada e em até 48 (quarenta e oito) horas. Caso não seja possível responder no referido prazo, a resposta deverá ocorrer em até 15 dias corridos, oportunidade em que a declaração deverá ser clara e completa, indicando a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados eventuais segredos comercial ou industrial.

O titular decidirá como as informações e dados serão fornecidos (meio eletrônico ou impresso); na hipótese de não haver especificação por parte do titular, os dados serão fornecidos por meio eletrônico.

Propósito/finalidade para utilização dos dados pessoais

Os dados pessoais são tratados para fins específicos, explícitos e legítimos (em consonância com esta Política) e não são processados de maneira incompatível com esses propósitos.

Quando a ABEP é controladora de dados pessoais, estes são processados principalmente para, mas não limitados, aos seguintes propósitos: gerenciamento de pesquisas, gestão de recrutamento, gestão de recursos humanos, contabilidade e gestão financeira, gestão de tesouraria e tributária, gestão de risco,

gestão de segurança de pessoal, gerenciamento de suporte de TI, gerenciamento de plataformas, gerenciamento de aplicativos, gerenciamento de segurança e saúde, gerenciamento de segurança de informações, gerenciamento de relacionamento com filiados, comunicação interna e externa, gestão de processos jurídicos, gerenciamento de projetos corporativos, cumprimento de obrigações contra lavagem de dinheiro ou quaisquer outros requisitos legais, operações de análise de dados, gestão corporativa legal e implementação de processos de *compliance*.

Para tanto, será necessário que no momento do fechamento e elaboração do Contrato, sejam considerados os seguintes pontos:

- Conteúdo do Contrato em Proteção de dados: (i) objeto do tratamento/processamento de dados, além de como se classificam as partes na relação contratual; (ii) natureza e finalidade do processamento; (iii) tipos de dados envolvidos; (iv) categorias de titulares de dados; (v) obrigações com direitos dos titulares.
- Em caso de operador, deve restar claro que este apenas age em consonância com as ordens lícitas do Controlador de Dados;
- Caso o operador pretenda subcontratar algum parceiro/fornecedor para atuar no fluxo de dados pessoais objeto do contrato, deverá: (i) verificar o nível de adequação à LGPD do subcontratado, exigindo sua adequação à presente política de privacidade da ABEP; (ii) dar ciência deste ato ao Controlador, por e-mail, possibilitando a este a oposição em relação ao parceiro subcontratado;
- O operador, apesar de não ser o responsável pelo canal de atendimento responsável pelo exercício dos direitos previstos na LGPD pelos titulares dos dados pessoais, deverá replicar as solicitações, quando requerido pelo Controlador, além de contribuir com informações solicitadas, dentro do possível;
- O operador deve auxiliar o Controlador em caso de incidentes a cumprir com as exigências de notificação da LGPD;
- Todas as partes envolvidas no fluxo de dados pessoais devem garantir a segurança do processamento, cada qual em seu ambiente;
- Ao final do contrato, o operador deverá excluir ou devolver todos os dados ao controlador, de acordo com a preferência deste, ressalvadas as hipóteses de tratamento obrigatório previstos em leis, regulamentos e portarias;
- Em caso de concessão de acessos com login e senha, o acesso deverá ser individual e de responsabilidade do usuário a quem foi confiado o acesso, sendo proibido o compartilhamento de senhas.

Processamento por terceiros sob orientação da ABEP

Caso terceiros realizem o tratamento de dados pessoais, em nome da ABEP, deverão essas empresas terceiras necessariamente respeitar obrigatoriamente todas as condições aqui estipuladas, as Políticas de Segurança da Informação e a legislação vigente referente ao assunto.

Armazenamento de dados em geral

A ABEP manterá os dados pessoais processados com precisão e, quando necessário, atualizados. Além disso, serão mantidos apenas dados pessoais pelo tempo necessário e para as finalidades para as quais são processados.

Armazenamento de dados por parceiros

No caso do armazenamento de dados pessoais por parceiros, será necessário que estes estejam em conformidade com a presente Política e legislação vigente acerca do tema de Proteção de Dados Pessoais.

Não será permitido o armazenamento de dados por parceiros dos quais não possuam o mesmo nível de segurança da informação e proteção de dados que a ABEP.

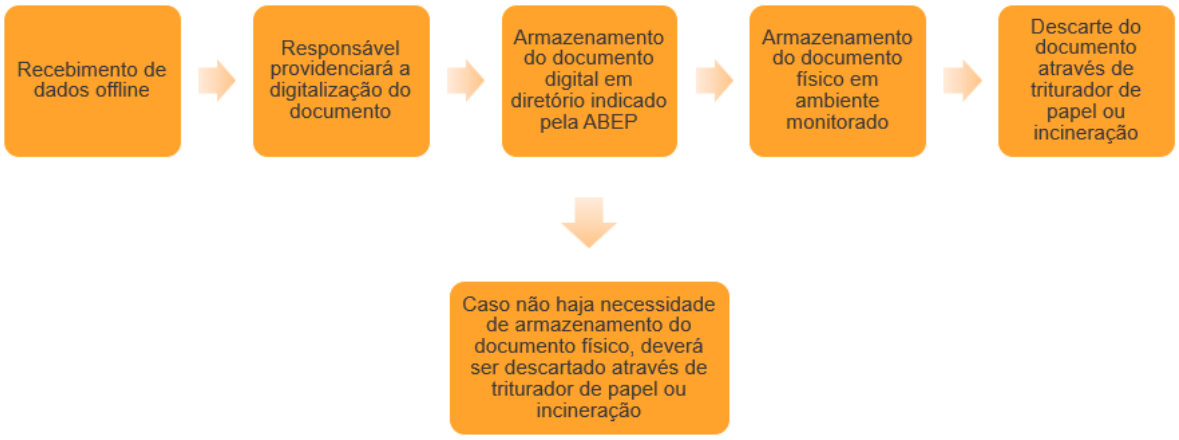
Armazenamento de dados físicos

O encarregado de dados e (ou) qualquer outra parte envolvida deverá se atentar ao armazenamento de dados físicos, realizados por meio de formulários em papel, fotocópias, dentre outros dados coletados de forma off-line. Em primeiro lugar, deverá o responsável avaliar a real necessidade da impressão do referido documento, sendo sempre que possível dar preferência para a visualização de documentos em formato digital.

O armazenamento deverá seguir o seguinte padrão: com o recebimento de dados através de meios off-line, deverá o encarregado providenciar a digitalização da documentação e disponibilizá-la em plataforma/diretório indicada pela ABEP para controle interno. Após digitalização, deverá o encarregado armazenar a documentação de forma segura conforme os padrões estabelecidos na presente política.

Os dados coletados por meio off-line deverão ser armazenados em ambiente monitorado, com acesso restrito a funcionários previamente autorizados, e deverão ser devidamente descartados, quando solicitado, ou pelo fim definitivo do tratamento do dado.

Caso não seja necessário o armazenamento da via física após digitalização, deverá o documento ser descartado. De mesmo modo, será necessário que o encarregado de dados e (ou) qualquer outra parte envolvida revise as informações armazenadas periodicamente, e no caso da identificação de informações com prazo expirado para descarte, deverá de imediato ser descartada nos moldes determinado abaixo.



O descarte do documento físico deverá ser feito de forma definitiva, através de triturador de papel ou incineração. O encarregado de dados deverá se atentar para que, após o descarte, a restauração do documento não seja possível.

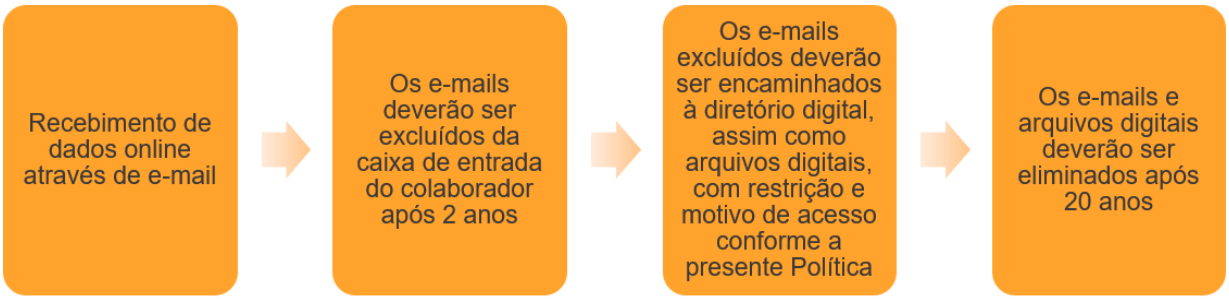
Armazenamento de informações digitais

O encarregado de dados e (ou) qualquer outra parte envolvida deverá se atentar ao armazenamento de dados digitais, inclusive e-mail.

O armazenamento deverá seguir o seguinte padrão: os e-mails deverão ser excluídos da caixa de entrada do colaborador após 24 (vinte e quatro) meses. A ABEP indicará diretório digital com restrição de acesso no qual todos os e-mails a serem excluídos da caixa de entrada dos colaboradores deverão ser arquivados (arquivo morto online). Este diretório apenas poderá ser acessado na hipótese de exercício regular de direito em contrato, processo judicial, administrativo e/ou arbitral.

Essa regra também aplica-se aos arquivos digitais que não tenham mais utilidade para o exercício das funções do(s) colaborador(es), ou seja, quando desprovidos de base legal para tratamento dos dados pessoais, quando do esgotamento da finalidade ou quando o titular solicitar a eliminação dos dados pessoais. Nessa hipótese, deverão os arquivos serem enviados para diretório digital com restrição de acesso.

Os arquivos digitais armazenados no diretório deverão ser eliminados após 20 (vinte) anos.



Será necessário que, o encarregado de dados e (ou) qualquer outra parte envolvida, revise as informações armazenadas periodicamente e, mediante identificação de informações com prazo expirado para descarte, imediatamente realize o descarte nos moldes acima determinados.

Retenção das informações

Os dados pessoais de usuários devem permanecer armazenados em ambiente seguro pelo período necessário para atender os objetivos previamente contratados com os titulares, pela ABEP, seus colaboradores, filiados, parceiros, fornecedores e prestadores de serviço. Quando solicitado pelo titular, a exclusão de seus dados deverá ser realizada, no prazo estipulado na seção referente aos direitos dos titulares, após comunicação, a não ser que o tratamento de dados tenha como fundamento base legal diversa do consentimento.

Caso os dados a serem excluídos tenham sido compartilhados com a ABEP, o responsável pelo compartilhamento deverá notificar a ABEP para que realize a exclusão dos dados também em sua base de dados.

Proteção de Dados e Recursos Humanos

O tratamento de dados pessoais coletados pela ABEP para a finalidade de controle da área de Recursos Humanos deverá acontecer em conformidade com a presente seção da política. Os dados tratados pelo RH terão a finalidade única e exclusiva de cumprir com as obrigações legais e procedimentais internas da ABEP relacionada à gestão de colaboradores, candidatos de processos seletivos e prestadores de serviços.

Processo Seletivo

No caso de aplicações submetidas de forma online ou física, será necessário que o RH, em conjunto com a área de Segurança da Informação, se atente aos seguintes critérios:

- O envio minimamente seguro das informações constantes das candidaturas, quando feitas através de aplicação online (ex. Criptografia);
- Caso a candidatura seja a candidatura encaminhada/aplicada em via física, será determinado um procedimento e responsável específico para encaminhamento e recebimento da informação, com prazo para tanto;
- Caso a candidatura seja analisada diretamente pelo superior da área, será necessário que esse colaborador seja orientado adequadamente sobre os cuidados na coleta e armazenamento das aplicações

Sobre a utilização de plataformas de recrutamento, em que todas as etapas do processo seletivo ocorram dentro da plataforma, desde a seleção do currículo até as entrevistas, o colaborador não poderá armazenar nenhuma informação obtida caso o candidato não seja contratado.

Em se tratando de plataforma de recrutamento responsável apenas pela seleção de currículos, sendo que todas as demais etapas do processo seletivo ocorram fora da plataforma (entrevistas e contratação), o colaborador, após a seleção do candidato, deverá descartar os documentos de forma a garantir que as informações nele constantes não sejam passíveis de recuperação; e em se tratando de documento eletrônico, deverá deletar os arquivos correspondentes àquela seleção, assegurando a impossibilidade de restauração.

Quanto aos currículos recebidos diretamente no e-mail do recrutamento do RH, após a primeira seleção de currículos, os demais não selecionados deverão ser deletados da caixa de entrada da caixa departamental.

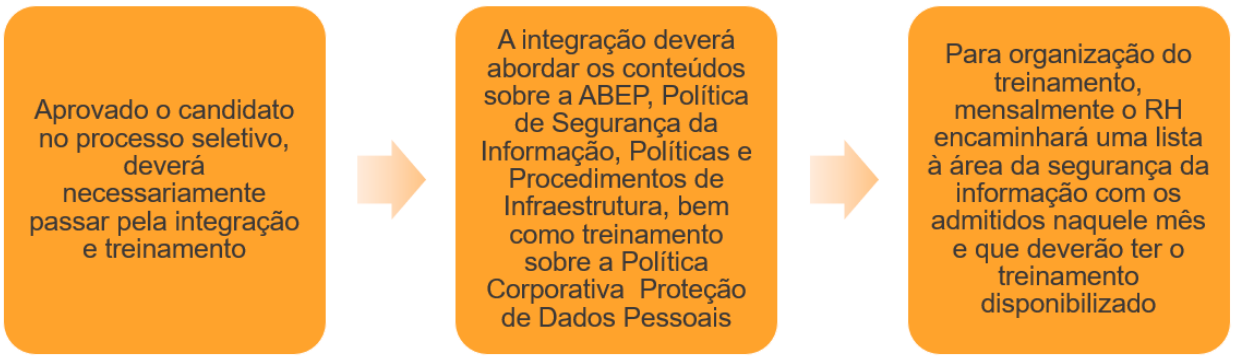
No caso de encaminhamento de currículos ao RH pelos colaboradores, estes deverão providenciar a exclusão do e-mail da caixa de e-mail no prazo de 01 (um) ano, ou preferencialmente, imediatamente após o encaminhamento. Caso o envio tenha ocorrido por meio de aplicativos de mensagens (ex.: WhatsApp), será necessária a exclusão do currículo do histórico do aplicativo.

Admissão

Aprovado o candidato no processo seletivo, será encaminhado exame admissional ao parceiro da contabilidade junto à ficha padrão, contendo as informações estritamente necessárias sobre o colaborador,

por e-mail criptografado e respeitados os critérios presentes na Política de Segurança da Informação. Será necessário que as informações do colaborador sejam armazenadas em diretório específico, na rede da ABEP, e o e-mail enviado deverá ser movido ao diretório digital com acesso restrito (arquivo morto online) da ABEP, a fim de evitar o armazenamento na caixa de e-mail do colaborador e em sua máquina.

O novo colaborador precisará, necessariamente, passar por um treinamento sobre a presente Política e sobre a temática de proteção de dados pessoais, bem como por uma integração, a qual contemplará conteúdos gerais sobre a ABEP, Política de Segurança da Informação, Confidencialidade e Políticas e Procedimentos de Infraestrutura.



Quando da adoção de procedimento que envolva a coleta de dados biométricos dos colaboradores da ABEP, os referidos dados somente serão utilizados em respeito à finalidade para a qual foram coletados e deverão ser descartados após o atingimento da finalidade.
No momento de sua admissão, ao colaborador deverá ser apresentado termo de uso de imagem e voz para campanhas, divulgações, teletrabalho (se for o caso), cursos, congressos, postagens realizadas pela ABEP (em redes sociais e revista), com a finalidade de lhe dar ciência sobre a possibilidade de utilização da imagem e voz por parte da ABEP, para o fim de campanhas, divulgações, cursos, congressos, postagens etc. e, eventualmente, monitoramento. Preferencialmente, que o termo de uso de imagem e voz conste no contrato de trabalho, ou que a concordância/assinatura seja manifestada no momento da assinatura do contrato.

Além disso, considerando que a ABEP realizará o armazenamento das informações do colaborador, deverá o RH possuir, dentro de sua área, procedimento documentado e específico para atendimento dos direitos dos titulares relacionados aos dados dos colaboradores. É recomendável a observância dos seguintes pontos:

- ❑ Indicação de responsável para responder tais questionamentos;
- ❑ Possuir um *checklist* para verificação rápida das informações do colaborador (com indicação de todas as bases utilizadas pelo RH) disponível somente para o responsável pela resposta;

- Garantir que todos os colaboradores tenham conhecimento sobre o responsável, e sobre o procedimento para garantia de seus direitos;
- Efetuar a resposta ao colaborador no período estipulado na sessão de direitos dos titulares;
- Possuir um mecanismo de checagem da identidade do solicitante dos direitos dos titulares (ex. Pedido pessoalmente no setor de RH);

Atestado médico

O colaborador deverá comunicar a sua ausência e enviar o atestado médico ao setor de Recursos Humanos, por e-mail. O setor de RH deverá arquivar o documento em diretório específico e protegido na rede e deletar da caixa de e-mail o arquivo recebido. Deverá, ainda, enviar o atestado médico à empresa parceira de contabilidade e deletar da caixa de saída o e-mail enviado.

Demissão

No caso de demissão do colaborador, todo o procedimento será realizado pelo parceiro de contabilidade. Uma vez finalizado, toda a documentação será enviada à ABEP, por e-mail, que armazenará em diretório específico do RH, com acesso restrito e o e-mail será movido ao diretório digital com acesso restrito (arquivo morto online). Eventuais documentos em posse do parceiro de contabilidade deverão ser destruídos conforme padrões estabelecidos na presente política.

Todas as contas do colaborador deverão ser desativadas, quando da demissão, e seu acesso físico à ABEP bloqueado.

Termo de Uso de Imagem, Nome e Voz

A ABEP se certificará, em todos os cursos, eventos, congressos e programações com as quais esteja envolvida, que houve a devida coleta de consentimento em Termo de Uso de Imagem, Nome e Voz dos participantes, parceiros, filiados, colaboradores e demais pessoas que estiverem presentes. Deverá, nesse Termo, constar a finalidade para a qual aqueles dados estão sendo coletados, bem como indicar, minimamente, sobre o tratamento que a ABEP e parceiros darão àqueles dados pessoais, tais como, publicações para divulgação dos eventos em redes sociais da ABEP ou diferentes formas de divulgação.

Atingida a finalidade para a qual a coleta ocorrera, os dados dos filiados, colaboradores, parceiros e participantes no geral, proveniente desses eventos, cursos, congressos e demais acontecimentos organizados pela ABEP, deverão ser descartados de modo que sua restituição não seja possível. A ABEP deverá garantir formas para que as pessoas que tenham manifestado “autorização” para uso de sua

imagem, nome e voz revoguem a cessão, podendo, inclusive, ser realizado por meio do Encarregado de Dados Pessoais da ABEP.

Aplicativos e Proteção de Dados Pessoais

O acesso às informações dos usuários do aplicativo da Revista ocorrerá apenas por pessoas autorizados, devendo os dados coletados para utilização do aplicativo serem o estritamente necessário para cumprimento da finalidade, bem como quais dados serão tratados. É essencial, ainda, que esta finalidade conste no contrato de prestação de serviços firmado com empresa parceira, juntamente às hipóteses de a ABEP compartilhar esses dados com terceiros.

A ABEP deve assegurar que no aplicativo conste a Política de Privacidade de Dados Pessoais de forma visível e acessível, permitindo maior compreensão e transparência quanto ao tratamento de dados dos titulares.

Será implementado calendário de eliminação de dados pessoais coletados para utilização do aplicativo, o qual deverá ser formalizado juntamente à empresa parceira, que deverá concordar com o procedimento e comprometer-se com os requisitos estipulados.

O ambiente de produção deverá ser segregado do ambiente de teste e homologação e apenas funcionários de TI com perfil de desenvolvedor poderão ter acesso às ferramentas de desenvolvimento.

Sistema CRQ

O contrato firmado entre a ABEP e empresa filiada deverá conter cláusula contratual que garanta à ABEP a licitude de origem dos dados que são inseridos na plataforma do CRQ, e que esses dados estão em conformidade com a finalidade descrita no objeto contratual. Além disso, sempre que a ABEP for realizar compartilhamento de dados, deverá ter essa hipótese em cláusula contratual, para dar ciência ao filiado sobre esse compartilhamento, de maneira clara e transparente.

Caberá à ABEP, junto à parceira responsável pelo gerenciamento do *software*, a adoção de ferramentas de armazenamento dos dados coletados na plataforma do CRQ, provenientes das pesquisas, de forma a cumprir com os requisitos legais. Quando não for possível a adoção de procedimento de exclusão desses dados, quando da desvinculação da empresa filiada à ABEP, que sejam adotados mecanismos de anonimização para as informações coletadas.

Classificação das informações pessoais a serem utilizadas

Todas as informações pessoais coletadas, tratadas e compartilhadas, em qualquer formato, devem ser classificadas pelo responsável pelo seu tratamento, observados os critérios ora criados e legislação nacional vigente, sendo certo que a sua classificação delimitará seu uso/finalidade e tratamento.

A classificação da informação é necessária para garantir que os dados recebam o nível adequado de proteção de acordo com sua criticidade e deverá ser realizada necessariamente quando da sua coleta, criação ou aquisição por seu proprietário.

O procedimento de classificação da informação deverá ser aplicado a toda informação da ABEP, não somente como procedimento padrão para alimentação dos sistemas, mas para todo tráfego de informação e, consequentemente, todo ciclo de vida do dado.

A classificação é segmentada nos três tipos de informação a seguir expostos:

#confidencial
Informações que possam influenciar o microambiente no qual a ABEP está inserida. São informações que devido a sua potencialidade deverá ser amparada pelo sigilo empresarial e comercial. Dentro da classificação “confidencial” estão abarcadas as classificações “sigiloso” e “setorial”, ambas, consideradas confidenciais na perspectiva da proteção de dados.

#interna
São as informações protegidas por alguma hipótese legal de sigilo, como comercial, profissional, industrial e segredo de justiça.

#pública
Informações que podem ser divulgadas sem restrições de acesso, observadas as conveniências do serviço a que diz respeito.

Critérios de tratamento da informação

Toda informação compartilhada ou veiculada deve ser classificada conforme a segmentação delimitada acima e deve ser tratada conforme os critérios abaixo delineados**:**

Informação em uso	#confidencial	#interna
Correio (serviço postal)	Uso desaconselhado. Caso necessário, recomenda-se o uso de correspondência ou remessa expressa que permita o rastreamento e aviso de recebimento.	Usar correspondência envelopada, registrada e que possa ser rastreada
Ambiente eletrônico	Utilizar canais que impossibilitem a interceptação das informações e manter registro das atividades, com adoção de mecanismos de criptografia ou outros controles equivalentes.	Utilizar canais que impossibilitem a interceptação das informações e manter registro das atividades, com adoção de mecanismos de criptografia ou outros controles equivalentes.
E-mail corporativo (destinatário interno)	Utilizar e-mail corporativo com criptografia ou sinalizar no assunto a necessidade de “manter em particular”.	Exclusivamente com uso dos veículos de comunicação administrativa
E-mail corporativo (destinatário externo)	Utilizar e-mail corporativo com criptografia ou sinalizar no assunto a necessidade de “manter em particular”.	Usar apenas quando houver interesse negocial, desde que autorizado pelo responsável
Mensageria, via mobile (WhatsApp, Microsoft Teams etc.)	Observar os veículos informativos de comunicação interna	Observar os veículos informativos de comunicação interna
Mensagem instantânea	Observar o uso dos veículos de comunicação administrativa	Observar o uso dos veículos de comunicação administrativa
FAX	Verificar a discagem correta do número, notificar o destinatário previamente ao envio e confirmar a recepção**.** Não utilizar para destinatários externos	Verificar a discagem correta do número, notificar o destinatário previamente ao envio e confirmar a recepção

Informação em uso	#confidencial	#interna
Sítios da internet	Não é permitido. Pode-se excetuar, mediante autorização formal do responsável pela informação.	Não é permitido. Pode-se excetuar, mediante autorização formal do responsável pela informação.
Conversas em locais públicos	Vedado	Vedado
Reuniões	Garantir que apenas pessoas autorizadas acessem o ambiente	Garantir que apenas pessoas autorizadas acessem o ambiente
Telefone fixo	Precaver-se contra a aproximação de pessoas não autorizadas. Não utilizar a função viva-voz, a não ser às portas fechadas	Precaver-se contra a aproximação de pessoas não autorizadas
Celulares	Precaver-se contra a aproximação de pessoas não autorizadas. Não utilizar a função viva-voz, a não ser às portas fechadas	Em locais públicos, utilizar longe de terceiros e com tom de voz moderado
Estações de trabalho	Estabelecer controle de acesso com restrição de usuário, controle de versionamento e senhas disponíveis nas ferramentas tecnológicas. Utilizar solução de criptografia, se possível	Utilizar controle de versionamento disponível nas ferramentas tecnológicas
Reprodução	Cópias devem ser previamente autorizadas pelo responsável pela informação. Atentar para a integridade e confidencialidade da informação	Permitido, desde que mantida a integridade das informações e seja para uso exclusivo no desenvolvimento das atividades profissionais

Informação em arquivo	#confidencial	#interna
Impressos, formulários e anotações	Guardar em local restrito e trancado, preferencialmente em armário de segurança. Acessível apenas aos que necessitam pela natureza do trabalho.	Guardar em local restrito e trancado. Disponível apenas aos que necessitam pela natureza do trabalho
Informações eletrônicas	Armazenamento em rede corporativa e sistemas que necessitem de autenticação do usuário e com controle de acesso compatíveis com a criticidade e confidencialidade da informação.	Armazenamento em rede corporativa e sistemas que necessitem de autenticação do usuário e com controle de acesso compatíveis com a criticidade e confidencialidade da informação.
Mídias removíveis e dispositivos móveis	Utilizar criptografia, guardar em armário de segurança. Disponível apenas aos que necessitam em razão da natureza de seu trabalho	Utilizar criptografia, guardar em local restrito e trancado. Disponível apenas aos que necessitam em razão da natureza de seu trabalho
Demais mídias	Guardar em armário de segurança. Disponível apenas aos que necessitam em razão da natureza de seu trabalho	Guardar em local restrito e trancado. Acesso apenas aos que necessitam em razão da natureza de seu trabalho

Descarte/ Destruição	#confidencial	#interna
Impressos, formulários e anotações com ou sem o logotipo ou qualquer identificação da ABEP	Utilizar fragmentadora ou qualquer outro meio, de forma a não permitir a sua recuperação.	Utilizar fragmentadora ou qualquer outro meio, de forma a não permitir a sua recuperação
CD, DVD, pen drive, HD externo e dispositivos móveis	Fragmentar, perfurar, picotar ou destruir, sobrescritas, de forma a não permitir sua recuperação	Fragmentar, perfurar, picotar ou destruir, sobrescritas, de forma a não permitir sua recuperação

Trabalho Remoto

Para que o colaborador realize suas atividades através do trabalho remoto, será necessária a assinatura de um Termo de Responsabilidade, quando da necessidade de transporte de equipamentos da ABEP.

Em se tratando de trabalho remoto em que o colaborador faça uso de máquina própria, a ABEP deverá, necessariamente, orientar esses colaboradores sobre o uso adequado das informações, de modo a

assegurar que o colaborador pôde compreender sobre todos os procedimentos de Segurança da Informação presentes nesta Política.

O colaborador em regime de trabalho remoto deverá:

- Obedecer a todos os padrões estabelecidos na Política de Segurança da Informação e da presente Política;
- Somente utilizar softwares aprovados para manipulação de dados pessoais;
- Considerar a confidencialidade das informações quando em discussões através de vídeo conferências, buscando sempre um lugar mais reservado, longe de pessoas;
- Caso se utilize de algum documento impresso, se atentar aos procedimentos de descarte dessa informação, sendo necessário que os procedimentos sejam reproduzidos independentemente do local;
- Ao fim do expediente, organizar todo conteúdo e equipamento relacionado a trabalho para evitar acessos indevidos;
- Ter atenção a links maliciosos e não utilizar pen-drives dos quais não tenha conhecimento sobre a procedência;
- Garantir que o equipamento utilizado está atualizado;
- Quando da utilização de equipamento próprio, não realizar *download*/salvar os arquivos da ABEP constantes na nuvem, em máquina própria;
- Em sendo necessária a realização de *download*, deletar, definitivamente, o documento baixado, imediatamente após o uso, de sua máquina própria.

Gerenciamento de senhas

Todos os acessos da ABEP precisam ser submetidos à controle por meio de login e senha individuais para cada colaborador, sendo que, caso identificado alguma operação ou área que realize o compartilhamento de credenciais, será necessária a comunicação à área de TI para remediação imediata da irregularidade.

As senhas são de responsabilidade direta do colaborador a quem foi confiado o acesso individualizado, e por isso as senhas são intransferíveis e confidenciais. O não cumprimento da confidencialidade do login e senha poderá implicar em medida disciplinar.

Caso o colaborador esqueça a sua senha, deverá entrar em contato com a área de TI para obter ajuda

Todas as senhas gerais deverão seguir o padrão mínimo de:

- No mínimo 8 caracteres;
- Conter caractere maiúsculo;
- Conter caractere minúsculo;
- Conter caractere especial;
- Não poderão conter sequências lógicas (ex. 1234);
- Previsão de troca de prazo máximo de 90 dias e mínimo de 1 dia;
- Não poderão ser reutilizadas qualquer uma das últimas 10 senhas.

Todas as senhas de usuários administrativos deverão seguir o padrão mínimo de:

- No mínimo 14 caracteres;
- Conter caractere maiúsculo;
- Conter caractere minúsculo;
- Conter caractere especial;
- Não poderão conter sequências lógicas (ex. 1234);
- Previsão de troca de prazo máximo de 45 dias e mínimo de 1 dia.

As senhas utilizadas para fins administrativos deverão ser armazenadas em cofre eletrônico.

É importante que as senhas de acesso não sejam anotadas e fixadas em locais de fácil acesso pelos colaboradores (ex. Anotados em papel adesivo e disposto no monitor do computador). Além disso, os prazos para previsão de troca de senha deverão ser observados por cada colaborador, e deverá ser reforçado pelas áreas responsáveis pela gestão de senhas na ABEP.

Acesso à rede

Todos os acessos na ABEP são controlados para impedir acessos não autorizados. No caso de desligamento, admissão, férias, dentre outras situações que necessitem alguma alteração nos acessos, deverá o RH informar imediatamente o setor de TI.

Caso algum colaborador verifique a possibilidade de acesso indevido a qualquer área/setor, deverá imediatamente informar o TI sobre tal irregularidade.

Deverá o setor de TI realizar uma revisão periódica (6 meses) de acessos, sendo possível a solicitação da revisão fora do prazo em caso de auditoria ou por solicitação da equipe de Segurança da Informação.

O pedido de solicitação de liberação de acesso deverá ocorrer através de e-mail com justificativa válida, período de liberação e permissão escrita do responsável pela área.

Deverá ser criado um inventário detalhado sobre os acessos aos bancos de dados, incluindo, principalmente, terceiros, filiado e parceiros, contendo, pelo menos, as seguintes informações sobre cada acesso: (i) data e hora; (ii) a duração; (iii) a identidade de quem acessa; e, (iv) o arquivo acessado.

Segurança

Implementamos medidas técnicas e organizacionais apropriadas para proteger os dados pessoais. Neste sentido, as áreas responsáveis pela segurança da informação devem seguir todos os controles estabelecidos para proteger as informações pessoais dos titulares contra perdas, mau uso, acesso não autorizado, divulgação, alteração e destruição.

Caso seja detectada a ausência de regulamentação de procedimento de algum aspecto da segurança da informação, a área de Segurança da Informação deverá ser imediatamente comunicada, por qualquer colaborador, a fim de que possa providenciar o desenvolvimento do procedimento e sua documentação.

Procedimento em caso de Incidente de Dados Pessoais

Caso seja detectado qualquer violação de dados pelas áreas de negócio, parceiros, filiados, colaboradores e terceiros da ABEP, essa deverá ser informada ao Comitê de Proteção de Dados Pessoais, imediatamente após conhecimento do ocorrido, a menos que seja capaz de demonstrar que essa violação não é suscetível de implicar em risco para os direitos e garantias individuais dos titulares de dados envolvidos. Na eventualidade de não ser possível essa comunicação ser imediatamente efetuada, a notificação deverá dar-se em até 48h, acompanhada dos motivos de atraso, podendo as informações serem fornecidas por fases sem demora injustificada.

A Comunicação deverá descrever: (i) a natureza da violação de dados (indicando categorias dos dados); (ii) as informações sobre os titulares de dados envolvidos; (iii) a descrição das prováveis consequências; (iv) descrever as medidas tomadas para atenuar a violação ou suas consequências.

O Comitê de Proteção de Dados Pessoais analisará a comunicação e, se for o caso, tomará as medidas legais cabíveis junto à autoridade competente.

Todos os contratos que envolverem compartilhamento de dados pessoais celebrados pela ABEP, deverão exigir da parte contrária que esta informe a ABEP sobre eventuais incidentes que envolvam os dados compartilhados, em até 24 horas.

Requisição de dados pela polícia e ordem judicial

A ABEP preza pela cooperação com as autoridades competentes a fim de garantir o estrito cumprimento das leis e a salvaguarda da integridade e segurança dos dados pessoais. Desta forma, exigimos a mesma postura de nossos parceiros.

A identificação da competência da autoridade para pedido de dados cadastrais deve ser feita sempre pelo jurídico.

Se solicitada à ABEP Informações Pessoais e esta não for a controladora destes dados, enviará prontamente ao Controlador de Dados aviso por escrito com prazo suficiente para permitir a este requerer eventuais medidas ou recursos apropriados.

Se solicitada, a ABEP revelará tão somente as informações que forem legalmente exigíveis e empreenderá seus melhores esforços para obter tratamento confidencial para as informações pessoais que foram reveladas.

Política de Privacidade e Contratos de Prestação de Serviços

A Política de Privacidade e Contratos de prestação de serviços devem conter os padrões de segurança adotados pela ABEP, bem como fazer referência ao cumprimento e observância desta Política e às instruções estabelecidas nas demais Políticas existentes.

A ABEP disponibiliza a Política de Privacidade em seu site como parâmetro mínimo, devendo todo o exposto nessa Política refletir a realidade da coleta e tratamento de dados realizada pelos seus parceiros.

Os parceiros deverão possuir Políticas de Privacidade em seus sites, que não excluam nem entrem em conflito com os requisitos e parâmetros estipulados na Política de Privacidade da ABEP. Em caso de divergência entre a Política de Privacidade dos Parceiros e da ABEP, prevalecerá a Política de Privacidade da ABEP.

Em último caso, na impossibilidade de desenvolvimento de Política de Privacidade própria pelos Parceiros, deverão estes replicar em seu site, ou possuir meios tecnológicos que direcionem o usuário para a política disponibilizada no site principal da ABEP.

Todos os contratos firmados devem possuir cláusulas específicas de proteção de dados pessoais, devendo a linguagem ser clara e simples (vide seção sobre Propósito/finalidade para utilização dos dados pessoais para mais informações sobre Contratos).

Caso se verifique que o parceiro não está de acordo com os padrões mínimos de segurança e proteção de dados estabelecidos na presente Política, deverá o Contrato firmado prever possibilidade de rescisão.

Conformidade e legalidade

Todas as áreas de negócio, parceiros, colaboradores e terceiros filiados à ABEP, devem necessariamente estar em conformidade com as leis e regulamentações vigentes e com os padrões de segurança estabelecidos nas demais Políticas disponibilizadas.

Resolução de Litígios

Qualquer dúvida ou preocupação com relação ao uso ou divulgação de informações pessoais deve ser encaminhada ao Encarregado de dados indicado pela ABEP. Este será o responsável por solucionar eventuais dúvidas, questionamentos e litígios acerca do uso e divulgação de dados pessoais de acordo com os princípios contidos nesta Política.

Proteção e uso Apropriado dos Bens e Informações da ABEP

Todos que tiverem acesso aos bens e informações de titularidade da ABEP são responsáveis pela proteção, uso e cuidados destes, sendo que qualquer suspeita de fraude, furto ou acesso desautorizado deve ser devidamente reportado para investigação.

O uso ou a distribuição desautorizada dos bens e/ou informações da ABEP violam esta Política Corporativa de Proteção de Dados Pessoais e podem resultar, além de sanções administrativas, em penalidades civis ou criminais.

Lealdade, Justiça e Transparência

Nós não coletamos ou processamos dados pessoais sem necessidade. Existem diversos motivos pelos quais a coleta e processamento de seus dados pessoais sejam necessários, como por exemplo, para a

execução de um contrato ou quando for necessário para o cumprimento de uma obrigação legal à qual estamos sujeitos ou quando necessário, mediante consentimento prévio.

Também podemos coletar e processar dados pessoais para os interesses legítimos da ABEP, exceto quando esses interesses forem anulados pelos interesses ou direitos e liberdades fundamentais do titular de dados pessoais.

Reconhecimento

A ABEP presume que seus parceiros, filiados e colaboradores tenham lido esta Política cuidadosamente, entendido seu conteúdo com a pretensão de cumpri-la, além de se comprometerem a incorporar em suas atividades tais valores. O desconhecimento desta Política não os exime das obrigações impostas.

Entre em Contato

Se você tiver dúvidas sobre a coleta e o processamento de seus dados pessoais pela ABEP, poderá enviar suas dúvidas ou reclamações seguindo o procedimento estabelecido nas declarações de privacidade que lhe foram comunicadas no momento da coleta de seus dados pessoais ou enviando um e-mail para o seguinte endereço: lgpd@abep.org .

Atualização

Podemos atualizar esta Política Corporativa de Proteção de Dados Pessoais oportunamente, à medida que surjam mudanças nos negócios ou requisitos legais. Se fizermos alterações significativas a esta Política, publicaremos um aviso em nossa Intranet quando as alterações entrarem em vigor e, quando apropriado, enviaremos uma comunicação direta a você sobre a alteração.

Período de Vigência

Esta Política Corporativa de Proteção de Dados Pessoais tem vigência por prazo indeterminado.

Por favor, clique aqui para confirmar ciência do conteúdo da Política Corporativa ABEP.

Através deste é necessário inserir alguns dados básicos de verificação e marcação da opção de leitura.

Caso não consiga clicar na opção citada acima, selecione o link: https://www.abep.org/politicaCorporativa/confirmacao.aspx